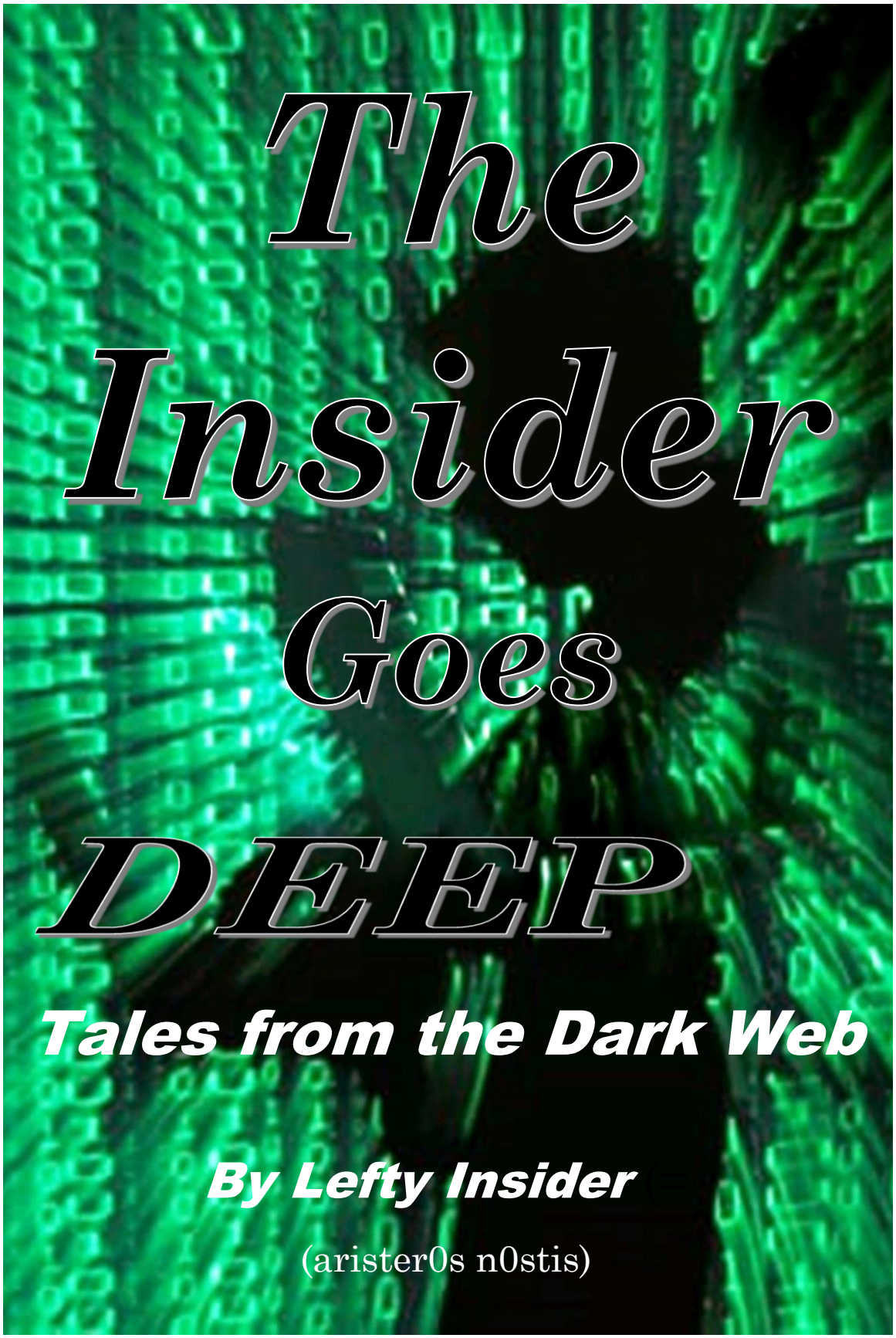

The Insider Goes DEEP
Tales from the Dark Web
By Lefty Insider
(arister0s n0stis)

The Insider Goes Deep

Target Market

This novel is targeted primarily to a demographic of 10 million college educated Baby Boomer aged men who are working in, or have worked in, the IT fields. The proposed goal of this manuscript is to reach one percent of this market, most of whom are not inclined to use social media, and find pdf files more accessible and readable than poorly formatted and weakly illustrated eBooks.

I want you, to go deep!

Acknowledgements
Those involved in the creation of this book, know who they are.

Editor and publisher
Last edited December 2022

ISBN number

U.S. Copyright Office
Copyright 1-4315250291
Case Date: 1/6/2017

This book is a work of historical fiction. Apart from the well-known actual people, events, and locales that figure into the narrative, all names, characters, places, and incidents are products of the writer's imagination or are used fictitiously.

Synopsis

This Insider Goes Deep title is a sequel to the writers' previous two books and follows the continued corruption of computer operating systems and software programs in supporting the devolution of the original Internet into an individualized predatory surveillance system, corporate ATM, and a global societal menace whose parasitic effects, and predatory behavior threaten lives, freedom, and democracy.

The Insider Trilogy plus one, is as follows:

Book One

- *The Insider (A Life Inside the Personal Computer)*

Approximately 98k words, 350 pages complete
Approximately 125 footnotes, 150 illustrations

Book Two

- *The Cozening (A Murder of Promise)*

Approximately 80k words, 300 pages complete
Approximately 100 footnotes, 200 illustrations.

Book Three

- *The Insider Goes Deep (Tales from the Dark Web)*

Approximately 120k words, 400 pages TBD
Approximately 50 footnotes, 200 illustrations
Approximately 200 CW links and 50 DW links
Approximately 30 Notes

And its companion book:

Book Four
A User Guide To The Dark Web
(The 42nd and Final Encyclopedia Cyberspacia)
Approximately 88k words, 400 pages TBD
Approximately 30 footnotes, 300 illustrations
Approximately 400 CW links and 200 DW links
Approximately 40 Notes

This is the third book and the finale in the trilogy, which collectively encompass a 50 year modern day Bildungsroman for the Lefty character and his life lived largely mediated by computer screens.

The fourth book in this series consists of the research work required to write this book, and is intended to be a reference book and an addition to the Dark Web Library of Imperial Trantor.

Like the previous two books, the third is a strong work and full of both literary and formatting innovations, and some computer geek humor. The two prequels to this book, an origin story named The Insider, builds background on the main character and the second, a middle story which picks up where the first left off chronologically and story wise. This final book in the series takes an unexpected direction for the main character. All are expected to be well received by the target demographic.

The Dark Web in reality consists of websites that exist in darkness, on overlay networks that use the Internet but require specific software, configurations, or authorization to access.

The Insider Goes Deep explores how through the Dark Web, private computer networks, and individuals, can communicate and conduct business anonymously without divulging identifying information, such as a user's profile and location. The Deep Web incorporates the Dark Web consisting of small, friend-to-friend peer-to-peer networks, as well as large, popular networks such as Tor, Freenet, I2P, and Riffle operated by public organizations and individuals.

This book seeks to answer the following questions, while both educating and entertaining the reader, with helpful information mixed with the comical stories and adventures of our main character.

The Dark Web (Net)

What is it?
Where is it?
How does it work?
How do you use it?
Who is there?
What are they doing?
Why are they doing it?

Are your passwords on a Post-it under your keyboard?

The books more technical Who, What, When and Where are told in the first person. However, Lefty's (n0stis/arister0s) adventures within this Dark Net hence the subtitle Tales from the Dark Web are told in third person, as are the semi humorous Insider stories.

A note to readers:

Throughout this book and the two previous prequels, this writer choose to write the term Internet with its original and intended initial capitalization spelling as a proper noun. This is also true for any outside imported text. The only exceptions are the Tales from the Deep Web forum and email messages that appear exactly as written, flaws and all. The Internet is a person, place, or thing and as we were all taught in grade school, requires proper capitalization. The trend in current print and online spelling as *lower case* which is disrespectful to its founders and creators in my view.

It is this writer's view that this intentional diminishment, via the lower case spelling, of this technological wonder and gift to humanity, is part of an effort by Corporate America to assimilate it into their Corporate Borg. To the founders, decentralization was the main idea, not the current walled gardens of Google (Alphabet), Apple, Amazon, Microsoft, and Facebook (META). While original pioneers like Vint Cerf may have been assimilated into the corporate Borg, people like Jon Postel and Tim Berners-Lee never were. Anyway, this writer gets to decide such things.

Non-original text formatting conventions

Text coming from "Websites" will be formatted thus.

Text coming from "Wikipedia" will be formatted thus.

Text coming from "News" sources will be formatted thus.

For purposes of clarity and the safety of your privacy, the following conventions of symbols are used throughout this book to identify web page hyperlink encryption: This will ensure that you know exactly where you are going on the Internet and what digital trail you are leaving behind.

Clear Web browser (.com, .org .gov, .io, .net, and country domain, etc.) http and mostly since 2013 and Snowden, encrypted https.

Dark Web (Tor) (.onion) always encrypted.

Note: this book is best read with a pdf reader and not a web browser, in Read Mode, and in portrait orientation which allows for both page turning and to zoom in on the graphics contained within. 1600x900 or higher screen resolution on a 24 inch monitor is recommended.

Note: any hyphens visible in the URL's are for text formatting purposes only. These links will function from this pdf if clicked on and not copied and pasted.

This book and the entire trilogy collection represent this writer's lifetime opus in the form of a modern day bildungsroman representing more than ten years of writing work and fifty years of research and life experience. As with my previous two books in this series, this one is part invented fiction, part historical fiction, part textbook, and part actual journalism.

These books are what Americans would call *edgy* or *antiestablishment* and contain what the Germans would call *Sturm und Drang*.[1]

> *In literature: a bildungsroman is a novel about the moral and psychological growth of the main character.*
>
> *Bildungsroman is the combination of two German words: Bildung, meaning "education," and Roman, meaning "novel." A bildungsroman is a novel that deals with the formative years of the main character, and with the character's psychological development and moral, (and in my case technological), education. The bildungsroman usually ends on a positive note, (perhaps this book is an exception to this) with the hero's foolish mistakes and painful disappointments over, and a life of usefulness ahead.*
>
> https://www.merriam-webster.com/dictionary/bildungsroman?src=search-dict-box

This book is dedicated to Sir Arthur C. Clarke and Isaac Asimov who have collectively inspired my writing.

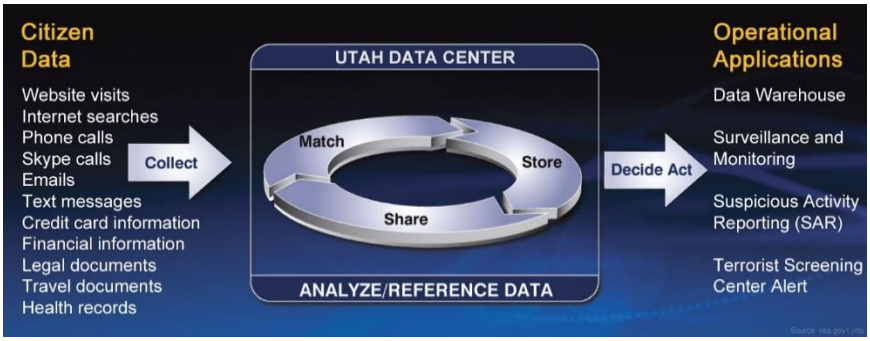
"Before you become too entranced with gorgeous gadgets and mesmerizing video displays, let me remind you that information is not knowledge, knowledge is not wisdom, and wisdom is not foresight. Each grows out of the other, and we need them all."
Sir Arthur C. Clarke (writer)

"Good writers copy, great writers steal." William Faulkner

[1] *A late 18th century German literary movement characterized by works containing rousing action and high emotionalism that often deal with the individual's revolt against society*

Foreword

Tired of fighting malware, data mining, and surveillance capitalism on the Clear Web, Lefty goes deep into the Dark Web to join up with like-minded computer geeks and freedom fighters to see what is happening there and to try to save the Internet, and freedom for all of humanity. (No small task.)



The NSA Collecting-Citizen-Data (graphic courtesy of Ed Snowden)

"One man scorned and covered with scars still strove with his last ounce of courage to reach the unreachable stars; and the world will be better for this." Cervantes, Don Qui9xote

Fair use rationale for illustrations & lyrics

This publication does not limit, nor claim to limit, the rights of the copyright holder. They remain the property and copyright of their owners.

Partial song lyrics are used as descriptive words.

Other graphics are either self-created, public domain via Wikimedia Commons, where attribution is not required, or come from the Creative Commons.

Images used are copyleft, screen shots, creative commons, Wikipedia or in the public domain. i.e.

https://www.pexels.com/search/darkweb/

Copyright disclaimer under Section 107 of the Copyright Act of 1976, allowances are made for “Fair Use” for purposes such as criticism, comment, news reporting, teaching, scholarship, and research. Fair Use is a use permitted by copyright statute that might otherwise be infringing. Non-Profit, educational, or personal use tips the balance in favor of Fair Use.

Table of Contents

Contents

The Insider goes DEEP

Target Market 1
Synopsis 2
A note to readers: 5
Foreword 7
Fair use rationale for illustrations & lyrics 8
Table of Contents 9
Prologue 12
Microsoft 22
Meta (Facebook) 24
Alphabet-Google (Android) 26
Apple 29
Amazon and Amazon Web Services (AWS) 36
Introduction 40
Chapter One, Deep Diving 49
Chapter Two, Dear Spectrum 55
Dear, Dear, Spectrum, the sequel 70
Dear, Dear, Dear Spectrum 82
Dear, Dear, Dear, and yet again Dear Spectrum 86
Ok Charter/Spectrum it is Time to Cut the Shit! 112
Charter/Spectrum Wisconsin IP assignments 128
How we got to where we are 132
BBS or Bulletin Board Systems 132
FidoNet 133
Gopher 134
Usenet 135
Newsgroups 136
CompuServe, Prodigy, and AOL 137
The Emergence Of The Internet and the Web 139
The Problems with the Clear Web 142
Pseudo Information Security 142
The Problems with Passwords 150

Solutions 154
DDoS 156
Distributed Denial-of-Service as a Service 156
SIM swap scam 157
SIM hijacking: 158
Some top 100,000 websites collect everything you type—before you hit submit 159
Navigating the Dark Web 161
When was the Dark Web invented? 161
Just How Deep is the Deep Web? 162
Are there bad things on the Dark Web? 162
Tales from the Dark Web 165
Part One: Who am I and why am I here? 165
Insider Story One </html> 182
Part Two: You don't have to go home, but you can't stay here. 192
Insider Story Two </html> 220
Part Three: What is happening here? 229
Insider Story Three </html> 259
Interlude 263
Part Four: Does anybody know what time it is? 265
Insider Story Four </html> 314
Part Five: A Place Online Without Identity 321
Insider Story Five </html> 361
Part Six: Where do we go from here? 364
The Cast of Characters 376
The Good Guys and Gals 376
The Bad Guys 378
Epilogue 379
Afterword 381
Further reading list 389
Publishing 390
Questions for the author 394
The Insider Writer website 396
Music Play List 398
The Heroes of our Time 402

Whistleblower Hall of Fame 402
Julian Assange 402
Ed Snowden 404
Chelsea Manning 406
Reality Winner 407
Thomas Drake 410
Bill Binney 411
Daniel Hale 413
Hero's Hall of Fame 415
Alan Turing 415
Sir Tim Berners Lee 415
Jon Postel 416
Ladar Levison 416
Robert William (Bob) Taylor 416
J. C. R. Licklider 417
George Pake 417
Jerome I. Elkind 418
David C. Evans 418
Jeff Rulifson 418
Douglas Engelbart 419
Theodor Nelson 419
Charles M. Herzfeld 420
Larry Tesler 420
Alan Kay 421
Norm Abramson 421
Judy Estrin 422
David Clark 422
Lawrence G. Roberts 423
Al Gore 423
Dave Crocker 424
Vannevar Bush 424
Paul Baran 425
Donald W. Davies 425
Leonard Kleinrock 426
Louis Pouzin 426
Stephen D. Crocker 427
Grace Hopper 427
Andy van Dam 428

Prologue

For mankind it was now at time of both the best and worst of life on this planet. Humanity rushed headlong into a parallel unsustainable cultural and scientific rise and as well as the slow death of their planet and almost certain demise of their future prospects.

For those newly born and the young, it was a time of great hope of continuing technological progress, the digital accessibility of the cumulative knowledge of all who came before. This information was available from a device in their pocket, or on their laps or desks. There was no longer an excuse to be stupid, yet too many in this society saw this trait of ignorance of the world around them as a superpower, and this disease had become endemic. There were major medical advances, and ambitious human exploration of the oceans and of space. Yet there were many who continued to choose superstition over science because it was easier on their small brains.

The wealthy who reveled in their decadence earned from their predatory thievery now having obtained a majority of the total money, engaged in the unaccountable plundering of the planet's resources and the eminent domain capture of the property of the world. Their corporations continued their Manifest Destiny of war driven empire building, war profiteering, dystopian global surveillance, and their parasitic digital data collection machines to exploit, commercialize, and commoditize human online life for limitless wealth. They passed this wealth from generation to generation, each generation believing that they were inherently smarter and more deserving. It was as if being born on third base carried with it the assurance, they had hit a standup triple. This was the primary source of their unwarranted and naïve optimism. With power and wealth, they have created their own personal narcissistic blue pill reality.

For all others, those matured and life experienced in the dirty ways of the world, it was a time of great dread from this unchecked parasitic vulture surveillance economics, the spread of division through racism, misogyny, Islamophobia, Xenophobia, classism, pandemic disease, and the man induced climate change self-destructing the world around them. The world was to them full of fools who did not understand that the essence of science is asking questions, collecting data, forming hypotheses for possible answers, and then revising these based on collecting and analyzing new data. The direct opposite of that are the more common superstition, speculation, theories, and beliefs.

The relentless driving of previously unknown levels of economic inequality

and unsustainable social division from parasitic and predatory behavior was all driven by the profit incentives of technology and social media corporations. By maximizing shareholder value and worshiping at the altar of Wall Street and quarterly profit increases, few saw this for the death cult it actually was.

The toll in human costs was immense from the immoral perpetual wars, autonomous robotic aerial executions perpetrating war crimes causing millions of civilian casualties early into this century, and the extra-judicial confinement, and torture of the innocent. They were confused by the magnitude of the fury of the continuing destruction of their planets environment, and the rise of political and religious fanaticism seeking a near-term biblical *end of days*. The acting out of those who have abandoned all hope, due to extreme poverty, high inflation, homelessness, and unemployment, led them to employ terrorism as a tool, and seek weapons of mass destruction.

The engineers and scientists emboldened by their successes and lack of accountability drove the society toward the danger of an uncontrollable autonomous artificial intelligence future. Governments have allowed cyber security exploits to be created, go unreported and unpatched for badly intentioned offensive purposes at the cost of defensive security. The CIA could no longer even secure their own offensive cyberwar hacking tools known by the WikiLeaks release as Vault 7. They intentionally and recklessly endangered everyone by throwing stones from a world full of glass houses. For the common man, these were the sources of their pessimism and their belief in a certain and undeniable destiny that would soon end the dominant species on their dying planet. For them, it looked increasingly like the end of civilization for the human race.

There were however, a few signs of hope that these same technologies could be employed on behalf of the have-nots and powerless. Scientific journalism as practiced by organizations like WikiLeaks[2] and some news outlets, and others, have had positive impacts for accountability, but at a high individual cost. The effects of requiring all media to link to the original source documents allowed the reader to judge for themselves if the reporters' interpretation is accurate and valid, and not disguised government propaganda. There were also the positive effects of increased use of end-to-end encryption in web traffic, data transfers, file, and email exchanges. This data scrambling reduced potential attack surfaces and the risk of data interception, profiling, and deanonymizing by malicious actors.

There were also some signs that the corporate media, due to the current political attacks and espionage threat punishments would place survival over

[2] *"Give a man a mask and he'll tell you the truth."— Oscar Wilde*

profit, as politicians sought to blur the line between whistleblower leaks and traditional journalism. This obscuration threatens their very survival, not to mention observance of the Constitutional protections, which allow democracies to exist. There was some hope that technology could be used to insist on consequences for bad behavior.

The rule of law and the accountability to it had come to be known as the operating system of a democracy.

In general, the moral physics that a near 250-year-old democracy had come to rely on had now failed them all, making this the worst of times for most, and degenerating each and every day.

Error code 155 is a malfunction in your systems operation

The prophecies of Idiocracy[3] swept through the analog and digital landscapes alike. Everyone's digital communications became cesspools of malware attempting to steal or hold for ransom your identity, your personal information and your money.

Citizens did not have any fear the social media that now unknowingly controlled them and mismanaged their brains. The Internet or Clearnet[4] was

[3] This film tells the story of an American soldier, who was part in a classified military human hibernation experiment, who accidentally awakens 500 years later in a dystopian society. There mankind has embraced anti-intellectualism and commercialism was rampant, and was devoid of intellectual curiosity, social responsibility, or coherent notions of justice and human rights.
[4] Clearnet is a term referring to the publicly accessible Internet, and the opposite of the DarkNet

now a dangerous place for those unaware to visit. Everything connected to this system was hackable. Hell, the NSA could not even protect their hacking tools from being stolen by crackers from the Shadow Brokers.

Billions of simple minded and uninformed humans acted like lemmings all stepping off digital cliffs and into the corporate clouds. There, their personal data being vacuumed like some giant corporate digital spider spinning its web and sucking dry anything that smelled like personal data from their monopolistic communication pipes containing the digital lives of billions of people on the planet. Yet these corporations did not care enough to protect this data from near daily intrusions and theft. Most of these were banks and medical data hosting companies that did not care enough to even offer two-factor authentication to their users, secure encrypted databases, or sufficiently defensive network infrastructures.

Medical care was being privatized from nonprofit hospitals and clinics to for profits with long wait times, substandard care, and their advertising screens in the waiting and exam rooms. "Collect it all" they said. "Data is just like money to us."

Yet corporations also used this data to alter the thinking, habits, purchases, and voting preferences of the masses in the now damaged and failing democracies. These mindless human drones continued to carry these tracking devices with them and placed additional surveillance devices in their homes, on themselves, and in their cars being misled by some misguided sense of convenience. They did this of course, because their connected surveillance devices told them to.[5]

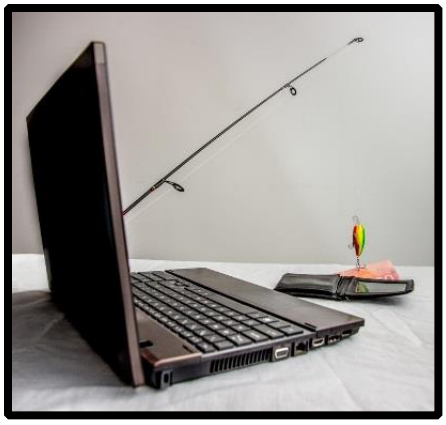
Those around the world now increasingly impoverished, unemployed, and without any hope from being on the wrong end of Western empire building, became criminals who sought out your money with phishing[6] emails. This was a land of one stop shopping for criminals. Data is really just like money now.

---

encrypted, anonymous services of the Tor network.

[5] "We watch the television, because it tells us that we should." Supertramp

[6] Phishing is an example of social engineering techniques being used to deceive users with communications purporting to be from trusted parties such as social web sites, banks, online payment processors, or IT administrators.



Phishing your wallet

Back in the early days of computers, no one had worried about all the disparate data being collected by these earlier computing machines, because the computer scientists knew, or thought they did, that there would never be a way to aggregate it all these disparate databases into anything collectively useful to anyone. But then came the unregulated profit incentives, which birthed server farms, and Internet clouds, web crawlers, bots, and the algorithms to find, manipulate, sort, and deliver this big data of a nation, and then of the entire world, to these corporations.

These early pioneers were wrong. Very, naïve and wrong.

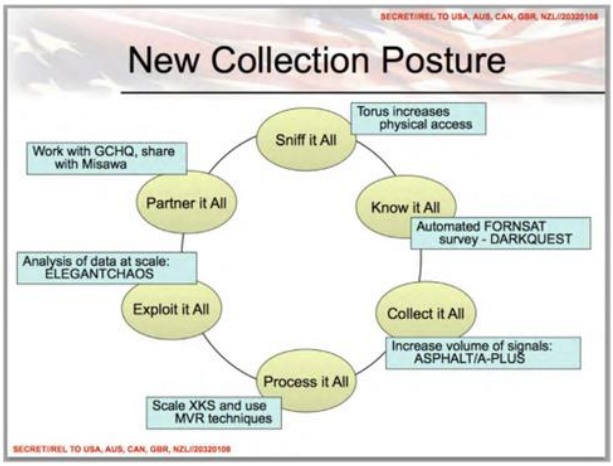
Greed was now good, and practiced from the top on down. People voted for politicians based on what was in it for them. They were disconnected from any remaining personal morals or ethics. It was hooray for me and screw you buddy! I got mine, now you try to get yours. The Haves pulled up all the ladders that they had used to get there, and any elevators was never sent back down. Every business transaction was seen as an opportunity to screw someone over.

Banks and money ruled as if some great vampire squid had wrapped itself around the face of humanity, relentlessly jamming its blood funnel into anything that smelled like money.[7]

And of course, the American National Security Agency or NSA was hoovering up all worldwide digital communications under the guise of Signals Intelligence (SIGINT). They used their significant computer power to translate all of these zeros and ones into Human Intelligence (HUMINT) to know everything about everyone. “Collect it all,” they said.

---

[7] *July 2009 Rolling Stone magazine "The Great American Bubble Machine," by Matt Taibbi*



NSA PowerPoint slides courtesy of the NSA via Edward Snowden

Why would the NSA be interested in you?

You are not much of a thinker are you?

You want someone else to decide what personal information that you share with the world?

The NSA is interested in ***everything and everyone***. They collect and analyze everything. Then they store it, mostly forever in their Utah datacenter. Information is power, power to control, power to manipulate, power to convict, power to frame.

- Are you willing to share your salary?

- How about your purchases?
- How about your sexual preferences?
- How about you medical conditions?
- How about your political beliefs?
- How about your religious beliefs?
- How about your friends and all their information?
- How about your travel locations?

The NSA was gathering all this information from everywhere. They could now paint a complete picture of your life, right or wrong. What you know, who you see, what you believe, where you go. They can learn how you learn, how you think, and who you are.

- If you know someone is watching, do you behave and speak differently? Did you as a kid, if your mom or dad were watching?
- Did you grow up in a small town or neighborhood where everyone knew who's kid you were? Did it change your behavior?
- Is this really, what you want for your children, and grandchildren?
- Do you want to be led by leaders, or ruled by rulers?
- Do you want a democracy be replaced by and totalitarian oligarchy driven by greed and corruption, or worse yet a corporate government driven by profit?

It was also a time of post-factual politics, where politician's spent their time trolling and gas lighting the media and the public with demonstrably false conspiracy theories, designed to create division, fear, and confusion. When challenged they backed down with nihilistic denials, alternate facts, and attempts to delegitimize the media with claims of fake news. When directly confronted they build strawmen, and used Whataboutism[8] to change the

8 Whataboutism, is a logical fallacy that attempts to discredit an opponent's position by

subject to something else.

Dishonest Propagandist now became the job title of many of our politicians and rather than serving the people who they hoodwinked into electing them. They did not actually do things that help people like creating jobs, finding markets for it products, providing healthcare, employment, affordable housing, and adequate and relevant educational opportunities.

TV newsreaders continued to explore the depths of division, derision, and tribalism, to see just how low they could go. They plumbed the depths of our worst angels. They tested the strength of the nation's founding principles, checks and balances, and now had a democratic society bulging at its seams.

They did it for money and power, fundraising for their campaigns, and their ratings on TV for advertising monies.

After forty years of disinvesting in public education, the population was now semiliterate, uninformed and now where being aggressively intentionally digitally misinformed, their minds mismanaged with psychological warfare techniques, and thus disinclined to believe in facts and science and instead clung to unsubstantiated beliefs (superstitions) and unproven and fact-less theories and opinions provided by random unqualified people on corporate social media. They no longer considered the source of the information they consumed. The past failures to fully fund the public education systems had led to a nation of lazy minds unable to keep up with the complexities and pace of modern society. They then withdrew from trying to understand the modern world, because it was simpler and easier to live a smaller less complicated world of their own with blinders on. These people with a narrow view of convenience over common sense will follow their cars GPS faithfully and drive into a lake and continue to place each newly invented surveillance device not only in their pockets but in their homes and cars as well.

---

changing the subject without directly refuting or disproving the original argument. A classic Soviet/Russian disinformation technique.

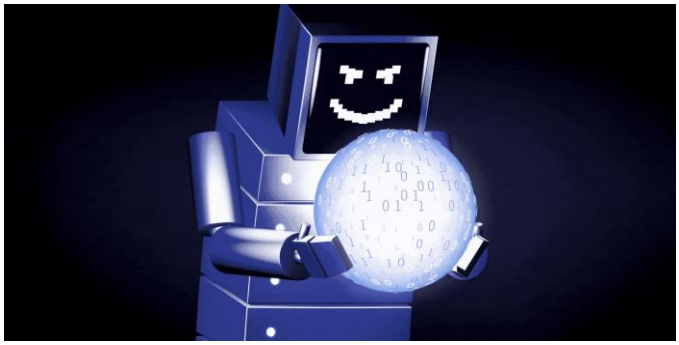


Image courtesy of theintercept.com

The Internet was purposely designed with intelligence at the end points, specifically with no centralized control. This came out of military operational continuity as well as university research personal and academic freedom perspectives.

But now these amoral and unbridled capitalist digital gangster corporations like Facebook (Meta), Google, Apple, Amazon, and Microsoft have inserted themselves as Internet gateways into every transaction and communication. More than 70% of all Internet traffic goes through sites owned or operated by Google or Facebook. Not unlike the Truman show[9], they are using tools and code to record everyone's digital lives, monitoring, guiding and predicting their behavior and wantonly and recklessly violating the American Constitutional guarantees of Life, Liberty, and the Pursuit of Happiness. They make their enormous profits from doing this socially disconnected, morally bankrupt, and conscience free work.

Does Liberty[10] include the freedom from being enslaved by machines that surround us?

"I'm sorry Dave, I'm afraid I can do that".

HAL 9000 from the movie 2001: A Space Odyssey.

The War Operation Plan Response, WOPR, "The only way to win a nuclear war, is not to play."

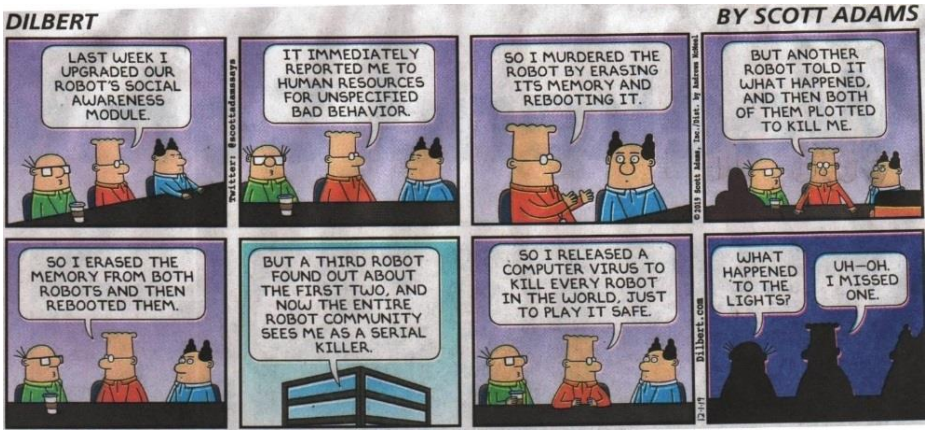
From the movie WARGAMES.

---

[9] The Truman Show is a film starring Jim Carrey as Truman, a man who grew up living an ordinary life that—unbeknownst to him—takes place on a large set populated by actors for a television show about him

[10] "Computers make excellent and efficient servants, but I have no wish to serve under them." -- Mr. Spock from Season 2, Episode 24 of the original Star Trek TV series.

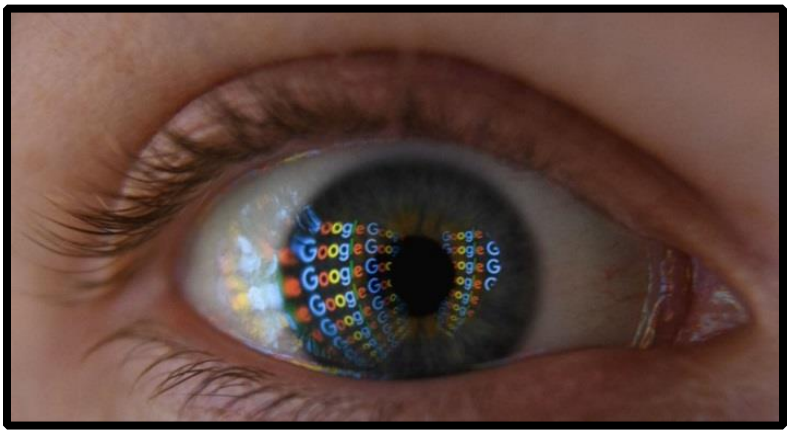
Meanwhile, back at the NSA…



Google has 10 million servers and is headed for 100 million. Facebook collects a staggering amount of data 500MB per person per day. (IBM estimate 2012) Facebook (Meta) is an Artificial Intelligence or AI pointed at your brain, using this monstrous amount of your personal data and the psychological warfare techniques (Cambridge Analytica) first developed to combat ISIS online recruitment. Yet this is the Faustian bargain[11] people are making, unwittingly for the most part.

Corporations had now overrun the government, which is now feckless and impotent in applying any kind of restraint or regulation. In previous decades, government restraint had been applied to IBM, AT&T, and Microsoft. But these corporations learned from this and now had massive numbers of lobbyists (outnumbering congressional members) spreading monies and offering jobs to get what they wanted. And they wanted unbridled operations.

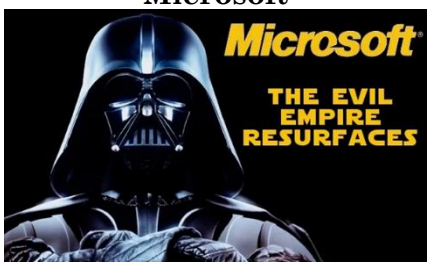
[11] *Faustian bargain, a pact whereby a person trades something of supreme moral or spiritual importance, such as personal values or the soul, for some worldly or material benefit, such as knowledge, power, or riches.*



These are the times in which we now live. Where corporations run roughshod over citizen's data privacy and these citizens are mostly oblivious to it.

Some highlights (lowlights) from some of the corporate evil doers follow.

Microsoft



Microsoft's Windows 10 required a Microsoft account (MSA) for telemetry tracking (keylogging) but you could bypass it if you knew how. Windows 11 requires an MSA to even run and now also requires a credit card number to even install.
Microsoft is testing promotions for some of its other products in the File Explorer on devices running its latest Windows 11 Insider build. From a report: bleepingcomputer.com. The new Windows 11 "feature" was discovered by a Windows Insider who saw an advertisement notification displayed above the listing of folders and files to the File Explorer file manager.
Microsoft could use ads to promote Microsoft products, for instance, about how to "write with confidence across documents, email, and the web with writing suggestions from Microsoft Editor. As you can imagine, the user reaction to this was adverse, with some saying that "File Explorer one of the

worst places to show ads," while others added that this is the way to go if Microsoft wants "people ditching Explorer for something else."

https://tech.slashdot.org/story/22/03/14/2036243/-microsoft-is-testing-ads-in-the-windows-11-file-explorer

Windows 11 users can expect to see warnings that their PC is not ready for Windows 11. Windows 11 will add a watermark on your desktop if your hardware is not supported

https://www.zdnet.com/article/windows-11-will-add-a-watermark-on-your-desktop-if-your-hardware-isnt-supported/

Annoying desktop watermark comes to users of unsupported Windows 11 PCs

It's only a watermark for now, but it's meant to encourage hardware upgrades.

https://arstechnica.com/gadgets/2022/03/annoying-desktop-watermark-comes-to-users-of-unsupported-windows-11-pcs/

Meta (Facebook)

Facebook Fails To Detect Hate Against Rohingya

Posted by msmash on Tuesday March 22, 2022 @11:30PM from the closer-look dept.

A new report has found that Facebook failed to detect blatant hate speech and calls to violence against Myanmar's Rohingya Muslim minority years after such behavior was found to have played a determining role in the genocide against them. The report shared exclusively with The Associated Press showed the rights group Global Witness submitted eight paid ads for approval to Facebook, each including different versions of hate speech against Rohingya. All were approved by Facebook to be published. The group pulled the ads before they were posted or paid for, but the results confirmed that despite its promises to do better, Facebook's leaky controls fail to detect hate speech and calls for violence on its platform. The army conducted what it called a clearance campaign in western Myanmar's Rakhine state in 2017 after an attack by a Rohingya insurgent group. More than 700,000 Rohingya fled into neighboring Bangladesh and security forces were accused of mass rapes, killings and torching thousands of homes.

On Feb. 1 of last year, Myanmar's military forcibly took control of the country, jailing democratically elected government officials. Rohingya refugees have condemned the military takeover and said it makes them more afraid to return to Myanmar. Experts say such ads have continued to appear and that despite its promises to do better and assurances that it has taken its role in the genocide seriously, Facebook still fails even the simplest of tests -- ensuring that paid ads that run on its site do not contain hate speech calling for the killing of Rohingya Muslims.

7 Ways Facebook Is Bad for Your Mental Health
How staying in touch may be driving you nuts.

https://www.psychologytoday.com/us/blog/sex-murder-and-the-meaning-life/201404/7-ways-facebook-is-bad-your-mental-health

Facebook Researchers Find Its Apps Can Make Us Lonelier (bloomberg.com) 31

Posted by msmash on Wednesday March 02, 2022 @10:45AM from the closer-look dept.

An anonymous reader shares a report: When Facebook hosted an internal competition a few years ago to develop new product ideas, a handful of employees teamed up to build a robot named Max. Shaped like a small, upside-down bowl, Max was designed to be a companion -- a physical device humans could talk to that could detect their mood, according to two people familiar with the hackathon project. The creators gave Max little ears and whiskers so the device would be more fun and approachable, like a cat. Max never evolved beyond the hackathon. But engineers and researchers at the company, now called Meta Platforms, are still grappling with the thorny problem the experimental robot cat was designed to combat: loneliness.

Meta, with a mission to help people connect online, has discovered through internal research that its products can just as easily have an isolating effect. As the company struggles to retain and add users for its already-massive social networks, making sure those people are happy is key to Meta's financial success. Loneliness has come into sharper focus at Meta during the Covid-19 pandemic, as people use its social media apps as alternatives to in-person experiences. Meta has promoted its role as a digital connector, running ads touting its groups and messaging products. "We change the game when we find each other," reads a tagline for one of its recent commercials. But internally, employees are questioning their products' impact on mental health.

Alphabet-Google (Android)

Android's Messages, Dialer Apps Quietly Sent Text, Call Info To Google (theregister.com)

> *Google's Messages and Dialer apps for Android devices have been collecting and sending data to Google without specific notice and consent, and without offering the opportunity to opt-out, potentially in violation of Europe's data protection law. From a report: According to a research paper, "What Data Do The Google Dialer and Messages Apps On Android Send to Google?" [PDF], by Trinity College Dublin computer science professor Douglas Leith, Google Messages (for text messaging) and Google Dialer (for phone calls) have been sending data about user communications to the Google Play Services Clearcut logger service and to Google's Firebase Analytics service.*
> *"The data sent by Google Messages includes a hash of the message text, allowing linking of sender and receiver in a message exchange," the paper says. "The data sent by Google Dialer includes the call time and duration, again allowing linking of the two handsets engaged in a phone call. Phone numbers are also sent to Google." The timing and duration of other user interactions with these apps has also been transmitted to Google. And Google offers no way to opt-out of this data collection. [...] Both pre-installed versions of these apps, the paper observes, lack app-specific privacy policies that explain what data gets collected -- something Google requires from third-party developers. And when a request was made through Google Takeout for the Google Account data associated with the apps used for testing, the data Google provided did not include the telemetry data observed.*

UK Government To Speed Up Criminal Sanctions for Tech Bosses With New Online Safety Laws (cnbc.com) 22

> *Posted by msmash on Thursday March 17, 2022 @12:22PM from the shape-of-things-to-come dept.*
> *Executives at companies like Meta, Google, Twitter, and TikTok could face jail time sooner than anticipated if they fail to cooperate with the U.K. Internet regulator, Ofcom. From a report: The U.K. government announced*

Wednesday that executives may face prosecution or jail time within two months of the new Online Safety Bill becoming law, instead of two years as it was previously drafted. The Online Safety Bill will be presented to lawmakers in Parliament on Thursday and could become law later this year. It aims to make it mandatory for social media services, search engines, and other platforms that allow people to share their own content to protect children, tackle illegal activity, and uphold their stated terms and conditions. The government said Wednesday that a range of new offenses had been added to the bill that makes the senior managers at tech firms criminally liable for destroying evidence, failing to attend or providing false information in interviews with Ofcom, and for obstructing the watchdog when it enters company offices.

Google Dupes Diners, Sidelines Restaurants For Delivery Profits (reuters.com) 49

Posted by BeauHD on Thursday March 10, 2022 @08:45PM from the deceptive-webpages dept.

Google has been making unauthorized pages for restaurants and using them to take a cut of fees from delivery orders through sites like Postmates, DoorDash, and Grubhub, according to a lawsuit Tuesday in San Francisco federal court. Reuters reports: The proposed class action (PDF) filed by Left Field Holdings, a Florida franchisee of Lime Fresh Mexican restaurants, said Google has been creating illegitimate digital "storefronts" for restaurants and deceiving users into thinking that the restaurants approved them. The lawsuit says Google takes a cut from the delivery sites for orders made through the storefronts, and in some cases delivery sites pay Google to divert users to them.

Left Field said restaurants are charged up to 30% of each order in fees by delivery sites, and therefore see "little (if any)" profits from them. Google never received permission to sell the restaurants' food, designed the storefronts to look like they were restaurant-approved, and placed a large "Order Online" button under restaurant search results to lure users to its storefronts, according to Left Field. [...] The lawsuit accuses Google of deceiving customers and violating federal trademark law starting in 2019. It asks for an undisclosed amount of money damages on behalf of Left Field and similarly affected restaurant owners and a ban on Google's alleged misuse of their trade names. In response to the lawsuit, a Google spokesperson said that the "Order Online" feature is meant to "connect customers with restaurants they want to order food from," and that it lets restaurants "indicate whether they support online orders or prefer a specific provider, including their own ordering website."

Google Routinely Hides Emails From Litigation By CCing Attorneys, DOJ Alleges (arstechnica.com) 64

Posted by msmash on Wednesday March 23, 2022 @06:01PM from the you-don't-say dept.

The US Department of Justice and 14 state attorneys general yesterday asked a federal judge to sanction Google for misusing attorney-client privilege to hide emails from litigation. From a report: "In a program called 'Communicate with Care,' Google trains and directs employees to add an attorney, a privilege label, and a generic 'request' for counsel's advice to shield sensitive business communications, regardless of whether any legal advice is actually needed or sought.

Often, knowing the game, the in-house counsel included in these Communicate-with-Care emails does not respond at all," the DOJ told the court. The fact that attorneys often don't reply to the emails "underscore[es] that these communications are not genuine requests for legal advice but rather an effort to hide potential evidence," the DOJ said. The DOJ made its argument in a motion to sanction Google "and compel disclosure of documents unjustifiably claimed by Google as attorney-client privileged" and in a memorandum in support of the motion. "The Communicate-with-Care program had no purpose except to mislead anyone who might seek the documents in an investigation, discovery, or ensuing dispute," the DOJ alleged.

Apple

Mac Studio Storage Not User-Upgradeable Due to Software Block (macrumors.com) 179

Posted by BeauHD on Tuesday March 22, 2022 @06:00AM from the classic-Apple-moves dept.

Despite being easily removable since it is not soldered down, the Mac Studio's SSD storage is not currently user-upgradeable due to a software block, YouTuber Luke Miani has discovered. MacRumors reports: Initial teardowns suggested that the Mac Studio's storage could be upgradeable since it is not soldered in place. Each Mac Studio contains two internal SSD slots, and the SSDs themselves can be freely swapped between the connectors. In a video on his YouTube channel, Miani tested if the Mac Studio's storage is user upgradeable in practice. Miani wiped the SSD of a Mac Studio, removed it from the machine, and inserted it into an empty SSD slot in another Mac Studio, but the Mac's status light blinked SOS and would not boot.

The Mac Studio recognizes the SSD, but Apple's software prevents it from booting, suggesting that this is a conscious decision by Apple to prevent users from upgrading their storage themselves. On its website, Apple claims that the Mac Studio's SSD storage is "not user accessible" and encourages users to configure the device with enough storage at the point of purchase. It now seems that the purpose of the easily replaceable storage is to aid repairs performed by authorized technicians, who likely will have software tools that enable the Mac Studio to boot from different internal storage. Since the prevention of user-upgradeability appears to simply be due to a software block, Apple could enable users to upgrade their own storage in the future via an update.

Explaining the Mac Studio's removable SSDs, and why you can't simply swap them out

To upgrade the Mac's SSDs, it helps to understand how they work.

https://arstechnica.com/gadgets/2022/03/explaining-the-mac-studios-removable-ssds-and-why-you-cant-just-swap-them-out/

Apple, Microsoft and Google All Receive Poor Grades on Repairability Report Card (theverge.com) 20

Posted by msmash on Tuesday March 08, 2022 @12:49PM from the closer-look dept.

Laptops and smartphones made by Apple, Microsoft, and Google are considerably less repair-friendly than those made by competitors Asus, Dell, and Motorola, according to a new report. From a report: These findings may be unsurprising to people who like to fix gadgets, but the data to back them up comes from an unusual source: the companies themselves. The report, released today by the US Public Research Interest Group's Education Fund, draws on data companies are now releasing in France to comply with the government's world-first "repairability index" law, which went into effect last year. The law requires manufacturers of certain electronic devices, including cell phones and laptops, to score each of their products based on how easily repairable it is and make that score, along with the data that went into it, available to consumers at point-of-sale.

Apple Hit With Sixth Antitrust Fine Over Dutch Dating Apps Payments (techcrunch.com) 29

Posted by msmash on Monday February 28, 2022 @01:27PM from the tussle-continues dept.

Apple still has not complied with a Dutch antitrust order to allow local dating apps to have the option to use third party payment tech to sell digital content to their app users. From a report: In a statement today, the Dutch Authority for Consumers & Market (ACM) said it has levied a sixth fine against the tech giant for non-compliance with an order first issued last year. The iPhone maker is now facing a $33.6 million penalty over the issue, with the prospect of further $5.6 million increases in the coming weeks if it continues to stonewall the regulator (up to a $56 million maximum).

Surveillance Firm Says Apple Is 'Phenomenal' For Law Enforcement (appleinsider.com) 34

Posted by BeauHD on Friday February 25, 2022 @09:25PM from the show-and-tell dept.

Secret recordings of a surveillance firm's presentation show how much iCloud data Apple surrenders to law enforcement with a warrant -- though it is Google and Facebook that can track a suspect to within three feet. Apple Insider reports: PenLink is a little-known firm from Nebraska, which earns $20 million annually from helping the US government track criminal suspects. PenLink also sells its services to local law enforcement -- and it is from such a sales presentation that details of iCloud warrants has emerged. According to Forbes, Jack Poulson of the Tech Inquiry watchdog attended the National Sheriff's Association winter conference. While there, he secretly recorded the event.

During the presentation, PenLink's Scott Tuma described how the company works with law enforcement to track users through multiple services, including the "phenomenal" Apple with iCloud. Apple is open about what it does in the event of a subpoena from law enforcement. It is specific about how it will not unlock iPhones, for instance, but it will surrender information from iCloud backups that are stored on its servers. "If you did something bad," said Tuma, "I bet you I could find it on that backup." Tuma also says that in his experience, it has been possible to find people's locations through different services, although not through iCloud. "[Google] can get me within three feet of a precise location," he said. "I cannot tell you how many cold cases I've helped work on where this is five, six, seven years old and people need to put [the suspect] at a hit-and-run or it was a sexual assault that took place." It is also possible for law enforcement and firms like PenLink, which help them, to get location data from Facebook and Snapchat.

[Apple Plans AirTag Updates to Address Unwanted Tracking (cnn.com) 43]

Posted by Editor David on Saturday February 12, 2022 @04:34PM from the thinking-different dept.

"Apple said Thursday it plans to add more safeguards to AirTags to cut down on unwanted tracking," reports CNN, "following reports that the devices have been used to stalk people and steal cars." In a blog post, Apple said it has worked with safety groups and law enforcement agencies to identify more ways to update its AirTag safety warnings, including alerting people sooner if the small Bluetooth tracker is suspected to be tracking someone. (Right now, it can take hours for an AirTag to chirp if it has been separated from its owner.) Other updates coming later this year include tweaking the tracker's tone sequence so the device is louder and easier to find, and allowing someone to see its distance and direction of an AirTag through the iOS precision finding tool. In addition, Apple will warn AirTag users during the setup process that tracking people without their consent is a crime.

That warning also reminds users "that law enforcement can request identifying information about the owner of the AirTag," Apple writes in their blog post: We have been actively working with law enforcement on all AirTag-related requests we have received. Based on our knowledge and on discussions with law enforcement, incidents of AirTag misuse are rare; however, each instance is one too many. Every AirTag has a unique serial number, and paired AirTags are associated with an Apple ID. Apple can provide the paired account details in response to a subpoena or valid request from law enforcement. We have successfully partnered with them on cases where information we provided has been used to trace an AirTag back to the perpetrator, who was then apprehended and charged. "We condemn in the strongest possible terms any malicious use of our products," Apple's blog post adds.

Daring Fireball supplies some analysis: The same features that help prevent AirTags from being used to stalk people without their knowing could also alert a thief that whatever it is they have stolen has an AirTag attached. There's no way for AirTags to serve both purposes, so Apple is increasing the protections against unwanted tracking, and emphasizing that AirTags are solely intended for finding your own lost items.

Apple's Grip On iOS Browser Engines Disallowed Under Latest Draft EU Rules (theregister.com) 41

Posted by BeauHD on Tuesday April 26

Europe's Digital Markets Act -- near-finalized legislation to tame the internet's gatekeepers -- contains language squarely aimed at ending Apple's iOS browser restrictions. The Register has received a copy of unpublished

changes in the proposed act, and among the various adjustments to the draft agreement is the explicit recognition of "web browser engines" as a service that should be protected from anti-competitive gatekeeper-imposed limitations. Apple requires that competing mobile browsers distributed through the iOS App Store use its WebKit rendering engine, which is the basis of its Safari browser. The result is that Chrome, Edge, and Firefox on iOS are mostly Safari.

That requirement has been a sore spot for years among rivals like Google, Mozilla, and Microsoft. They could not compete on iOS through product differentiation because their mobile browsers had to rely on WebKit rather than their own competing engines. And Apple's browser engine requirement has vexed web developers, who have been limited to using only the web APIs implemented in WebKit for their web apps. Many believe this barrier serves to steer developers toward Apple controlled native iOS app development.

The extent to which Apple profits from the status quo has prompted regulatory scrutiny in Europe, the UK, the US, and elsewhere. Now those efforts have been translated into the text of the DMA, which, alongside the Digital Services Act (DSA), defines how large technology gatekeepers will be governed in Europe. In short, when the DMA takes effect in 2024, it appears that Apple will be required to allow browser competition on iOS devices. "The potential for a capable web has been all but extinguished on mobile because Apple has successfully prevented it," said Alex Russell, partner program manager on Microsoft Edge who worked previously as Google Chrome's first web standards tech lead. "Businesses and services will be able to avoid building 'apps' entirely when enough users have capable browsers."

"There's a long road between here and there," he added. "Apple has spent enormous amounts to lobby on this, and they aren't stupid. Everyone should expect them to continue to play games along the lines of what they tried in Denmark and South Korea."

Apple Sued for Allegedly Deceiving Users With Privacy Settings (gizmodo.com) 29

Posted by EditorDavid on Saturday November 12, 2022 @03:34PM from the iPhone-home dept.

"Apple is facing a class action lawsuit for allegedly harvesting iPhone user data even when the company's own privacy settings promise not to," reports Gizmodo: The suit, filed Thursday in California federal court, comes days after Gizmodo exclusively reported on research into how multiple iPhone apps send Apple analytics data, regardless of whether the iPhone Analytics privacy setting is turned on or off. The problem was spotted by two independent researchers at the software company Mysk, who found that the Apple App Store sends the company exhaustive information about nearly everything a user does in the app, despite a privacy setting, iPhone Analytics, which claims to "disable the sharing of Device Analytics altogether" when switched off.

Gizmodo asked the researchers to run additional tests on other iPhone apps,

including Apple Music, Apple TV, Books, and Stocks. The researchers found that the problem persists across most of Apple's suite of built-in iPhone apps....
In the tests, turning the iPhone Analytics setting off had no evident effect on the data collection, nor did any of the iPhone's other built-in settings meant to protect your privacy from Apple's data collection. Mysk's tests on the App Store found that Apple receives that data along with details that can identify you and your device, including ID numbers, what kind of phone you're using, your screen resolution, your keyboard languages and how you're connected to the internet — the kind of information commonly used for device fingerprinting.

Your iPhone may be collecting more personal data than you realize
By Joe Maring
November 21, 2022
It's widely believed that iPhones are among the most secure smartphones you can buy — and that's largely true. But what if your iPhone was collecting more personal data about you than you were led to believe? According to security researchers Tommy Mysk and Tala Haj Bakry, that's exactly what's happening.

Your iOS app may still be covertly tracking you, despite what Apple says
Apple's landmark App Tracking Transparency may not be as tough as some people think.
Last year, Apple enacted App Tracking Transparency, a mandatory policy that forbids app makers from tracking user activity across other apps without first receiving those users' explicit permission. Privacy advocates praised the initiative, and Facebook warned it would spell certain doom for companies that rely on targeted advertising. However, research published last week suggests that ATT, as it's usually abbreviated, doesn't always curb the surreptitious collection of personal data or the fingerprinting of users.

Apple Exaggerations (lies)

Apple CEO Steve Jobs announced the new MacBook Air, at the Macworld Conference and Expo in San Francisco, Tuesday, January 15, 2008. The laptop billed as the world's thinnest computer features a 13.3" widescreen. While it fit in an envelope, so did the Sony VAIO PCG-505 that many had been using for a few years already. The Sony VAIO X505 was the current 505 at the time of the MacBook Air launch. The MacBook Air was 0.16-0.76" H x 12.8" W x 8.94" D and 3 pounds, whereas the X505 was 10.2 (W) x .38(front) - .8 (rear) (H) x 8.2 (D) and 1.73 pounds.

"Wozniak simply built the kind of computer that he personally wanted using available parts."

While true, what he built could not be mass-produced and the whole motherboard had to be redesigned by HP and others for actual production. This includes the chip layout for which he is given so much credit.

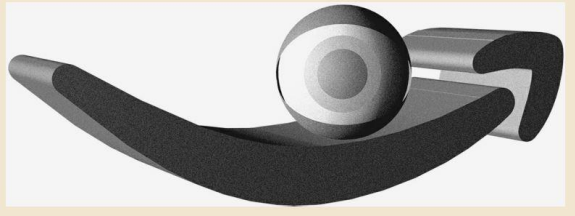
https://www.computerhistory.org/revolution/personal-computers/17/297

"Apple made the first and best selling personal computer"

Like many stories (propaganda) related to Apple. The actual truth lies elsewhere.

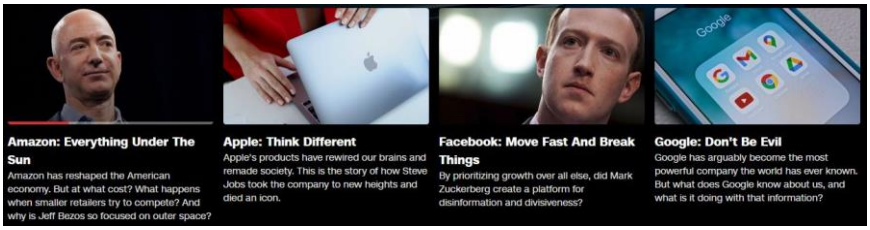
https://en.wikipedia.org/wiki/History_of_personal_computers#The_beginnings_of_the_personal_computer_industry

Amazon and Amazon Web Services (AWS)



Like the other monopolists Microsoft, Apple, Facebook, and Google, Amazon got to where they are by buying up their potential competitors.

They all have overrun the government and the Sherman Antitrust Act.



Four out of the five monopolists stealing from you

The Supreme Court Just Made a US-EU Privacy Shield Agreement Even Harder (thehill.com) 55

Posted by msmash on Wednesday March 23, 2022.

The U.S. Supreme Court's decision this month in FBI v. Fazaga, a case challenging FBI surveillance, will make it significantly harder for people to pursue surveillance cases, and for U.S. and European Union (EU) negotiators to secure a lasting agreement for transatlantic transfers of private data. The Hill reports: The justices gave the U.S. government more latitude to invoke "state secrets" in spying cases. But ironically, that victory undercuts the Biden administration's efforts to show that the United States has sufficiently strong privacy protections to sustain a new Privacy Shield agreement -- unless Congress steps in now. In July 2020, the EU Court of Justice (CJEU) struck down the EU-U.S. Privacy Shield, a legal framework used by thousands of U.S. companies to facilitate data transfers, because the U.S. failed to provide adequate protection for data belonging to people from the EU. Specifically, the court found that U.S. surveillance authorities, including Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, permit unjustifiably broad government surveillance. The court also found that the Privacy Shield failed to provide adequate redress mechanisms for Europeans whose data is transferred to the U.S. -- namely, the ability to be heard by an independent court that can order binding remedies. In striking

> *down Privacy Shield, the CJEU was clear: no EU-U.S. data-transfer agreement will survive the court's scrutiny until the U.S. narrows the scope of its surveillance and ensures that individuals subject to potentially illegal surveillance have a real, meaningful way to pursue accountability.*

Jack Dorsey Regrets His Role in Corporations Centralizing Discovery and Identity (twitter.com) 60

> *Posted by Editor David on Saturday April 02, 2022 @05:02PM from the looking-back dept.*
> *Twitter co-founder/former CEO Jack Dorsey made a remarkable statement Saturday on Twitter. "The days of Usenet, IRC, the web...even email (with PGP)...were amazing.*
> ***"Centralizing discovery and identity into corporations really damaged the Internet.***
> *"I realize I'm partially to blame, and regret it." Within two hours, his statement had been retweeted or quote-tweeted 4,700 times — while his original tweet drew 22,900 likes (and attracted over 2,000 comments). But it's not clear why 45-year-old Dorsey is reflecting nostalgically on 1990s-era bulletin board and chat technologies.*
> *The only thing in the news today about Jack Dorsey is a small blurb from The Information linking to a larger (paywalled) article titled "Jack Dorsey, Marc Andreessen and the Makings of a Crypto Holy War" The war of words, blocks, and memes between Jack Dorsey and Marc Andreessen wasn't only fascinating because of the billionaire egos at play. They really did seem to be grappling with an important question: Is there a superior economic system waiting to be rolled out, and if so, who should control it...? [T]he debate was an important one, with roots in both men's pasts and hints of a continuing war between Dorsey's Bitcoin maximalists and Andreessen's "crypto polyamorists."*

Wow, is that a regret I smell? Or just an attempt at redemption for Wall Street's ears, prior to his next invasion of privacy revenue generating venture?

Google, Microsoft, and Apple have designed their operating systems to facilitate the process of turning your personal information into a revenue stream for them. Amazon and Facebook, banks, real estate companies, and corporations in general capture and steal your data at an alarming rate. This is not simply a question of advertising: the extent of the personal data accumulated for the purpose of marketing is truly staggering, and has increasing consequences in our everyday lives, including health care, insurance, credit, immigration, and incarceration. Corporations are not solely to blame here, there are also some other bad actors involved in this problem.

https://www.dragos.com/

Ask yourself if these groups could operate effectively without the data and hacking tools that corporations, and governments have hoovered up, use, and cannot effectively safeguard.

According to Dragos, the most active threat groups targeting critical infrastructure are:

> ***Parasite:*** *a group which targets utilities, aerospace and oil and gas in Europe, the Middle East and North America. The group uses open source tools and known vulnerabilities for initial access. Parasite is suspected to be linked to Iran.*
> ***Xenotime:*** *a group which targets oil & gas companies in Europe, the United States and Australia. It's believed the group is linked to Russia.*
> ***Magnallium:*** *a group which initially targeted oil and gas and aircraft companies in Saudi Arabia, which has expanded targeted to Europe and North America. It's thought to be related to APT 33, a state-sponsored Iranian hacking group.*
> ***Dymalloy:*** *a group which targets electric utilities, oil and gas and other advanced industrial entities across Europe, Turkey and North America. Described as "highly aggressive", Dymalloy looks for long-term persistence in networks and is thought to be linked to Russia.*
> ***Electrum:*** *this group is capable of developing malware that can modify and control OT procedures and Dragos researchers say this operation was responsible for Crash Override – also known as Industroyer – a malware attack on Ukraine's power grid in December 2016. Electrum is associated with Sandworm, an offensive hacking operation that's part of Russia's GRU military intelligence agency.*
> ***Allanite:*** *a group which targets enterprise and OT networks in the UK and US electricity sectors, as well as German industrial infrastructure and uses access to conduct reconnaissance on networks to potentially stage future disruptive events. It's believed Allanite is linked to Russia.*
> ***Chrysene:*** *Active since at least 2017, this group has targeted industrial organisations in Europe and the Middle East, and mainly conducts intelligence gathering operations to potentially facilitate further attacks. Chrysense is suspected to be linked to Iran.*
> ***Kamacite:*** *a group which has been active since at least 2014 and believed to be responsible for cyber-attacks against Ukrainian power facilities in 2015 and 2016. The group is linked to Sandworm.*
> ***Covellite:*** *a group which has targeted electric utilities in Europe, the US and East Asia using malicious attachments in phishing emails. The group is thought to be linked to the Lazarus Group, a state-backed hacking group working out of North Korea.*
> ***Vanadinite:*** *A hacking group which targets external-facing, vulnerable software in industrial organisations around the world. It's thought to be linked to APT 41, a state-sponsored Chinese hacking operation.*

So it seems that these days that it is just one damn thing after another. Or perhaps as Roseanne Roseannadanna[12] would have said: "It's always something!"

"Most people are fools, most authority is malignant, God does not exist, and everything is wrong." Ted Nelson (pioneer of information technology, philosopher, and sociologist)

"They want to know how much you will pay for what you used to get for free" Tom Petty

[12] https://www.youtube.com/watch?v=9hYGtXIqDa0

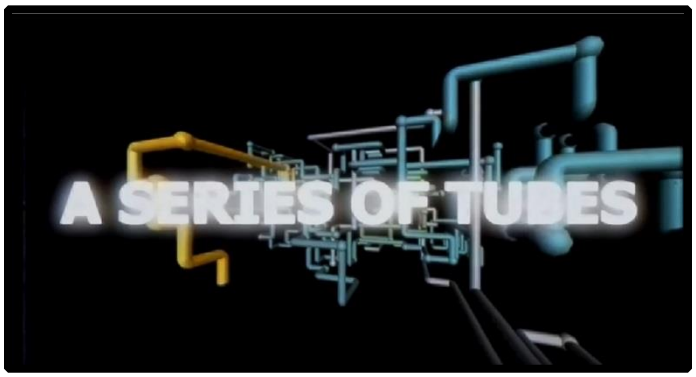
Introduction

Note: WOW! Well that Prologue was certainly a lot to absorb was it not. Now that the premise of the book is set, let me begin to tell the rest of the story.

The World Wide Web also called the Surface Web or Clear Web (mostly not encrypted[13], thus clear), is a *part* of the Internet. It is not as some think THE INTERNET and as such is Facebook, Google, Apple, Amazon and Microsoft are just parts of the whole. It is now more than a billion websites that a typical search engine used now by more than three billion worldwide users. You access it with a web browser such as Microsoft Internet Explorer, Microsoft Edge, Google Chrome, Safari, Pale Moon, Brave, or better yet Mozilla Firefox.

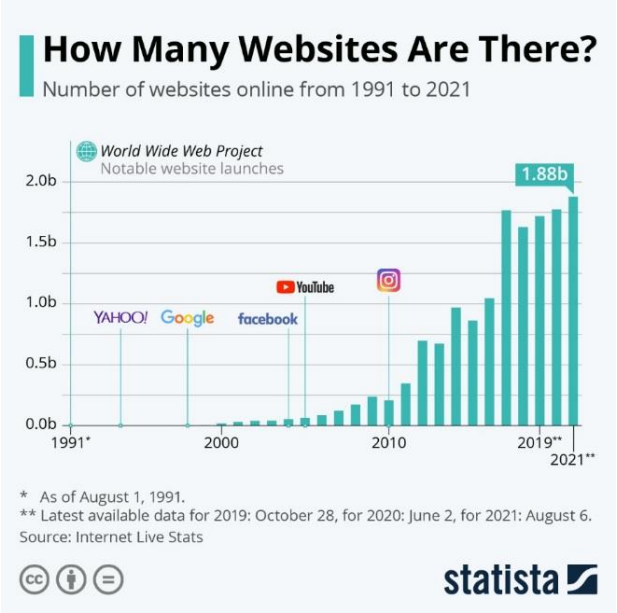
[13] *Encoded to prevent easy viewing.*

What the Internet in general is not is:



Although some of the unenlightened have been known to call it this.

The Deep Web, and we are talking about Deep not Dark here, is also a part of the Internet, and is anything that a standard search engine cannot access outside the enormous one billion; some estimates are as high as four billion, or so websites existing on servers around the globe. Spiders or also called bots crawl the surface web to populate the search engine databases but cannot effectively reach into the Deep Web.



Deep Web content can be found almost anytime you navigate away from a typical search engine and do a search directly in a website. Government databases and libraries contain huge amounts of Deep Web data. Searching the archives of a newspaper is an example of the Deep Web. It can also mean that their router settings have deliberately or accidentally made accessing these hosts virtually impossible. Some estimates put this part of the Internet at 400 to 500 times larger than the Surface Web.

For example if you navigate to www.ssa.gov and login, it will take you to https://secure.ssa.gov/mySSA/start

This is a secure https[14] site in the Deep Web.

What the Deep Web consists of are some of the things you cannot find on the Surface Web.

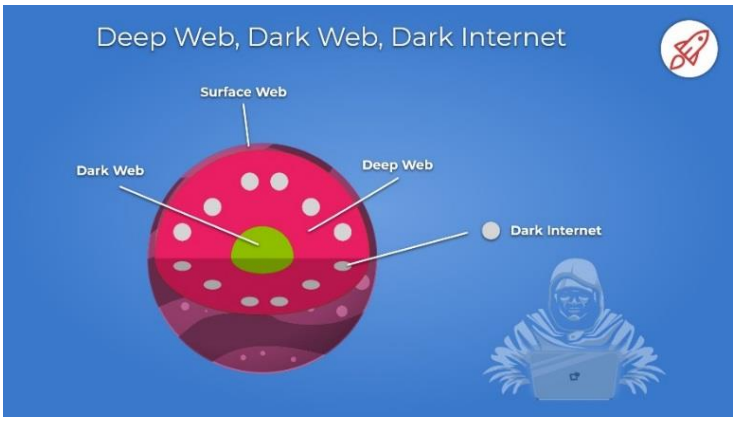
- Password protected pages.
- Attendance records, medical certificates etc.
- Bank records
- Encrypted Chat Messages (WhatsApp, Facebook Messenger etc.)
- E-mails sent between users
- Purchase-requiring content when not indexed on Search Engines (songs/ videos, school courses, etc.)

[14] *Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network.*

So in a nutshell, the content that exists on the Internet, but cannot be accessed via Search Engines, or requires special permission, is Deep Web content.

Some websites also intentionally "de-index" themselves, so that they can only be accessed by people who know the exact URLs, (addresses) these websites too are a part of the Deep Web, and host thing such as harmless discussions on conspiracy theories, and other such stuff.

Some refer to this as The Dark Internet and is similar to the Dark Web but actually is web data that is specific to one particular niche that users want to keep private. This is usually raw data used by scientists and researchers who want to keep the data private and untraceable.



As you may have guessed by now, not all un-indexed content is "illegal" or harmful, which further enforces my statement that the Deep Web is not illegal, it is purely "non-indexed" content, nothing more.

There is a parallel Internet you may not have run across yet only accessed by a special Dark Web browser and home to a freewheeling collection of sites for everything from anonymous activism to illicit activities. Not to mention regular people who do not wish to be surveilled.

The Dark Web (sometime called the DarkNet) is a small portion of the Deep Web that has been intentionally hidden and is inaccessible through standard web browsers. Dark Webs or hidden site, include Freenet[15] and Tor (The Onion Router).

---

[15] *Freenet is a peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the Web without fear of censorship. It uses your storage and bandwidth.*

https://www.torproject.org/ The Tor network is an anonymous network that can only be accessed with a special web browser, called the Tor browser. The websites limited to the Tor network have a special .onion address extension like darkweba6le5w52w.onion. Due to this, Tor's Dark Web is also known as onionland. It is an encrypted network built on top of the existing Internet. This is the portion of the Internet most widely known for illicit activities because of the anonymity associated with the Tor network. Although the Dark Web has some nebulous uses, most uses are innocuous. For example, people who want to communicate and associate online without fear of being shut down by a government agency. The Dark Web is much smaller than the Deep Web, and it is made up of numerous types of sites like crypto currency markets, The Hidden Wiki, and porn sites. It is perhaps most notorious for its anonymous marketplaces that often sell illegal products like drugs, fake documents, and weapons.

A Dark Web is any overlay network that can be accessed only with specific software, configurations, or authorization, often using non-standard communications protocols and network ports. Two typical Dark Web types are friend-to-friend networks (usually used for file sharing with a peer-to-peer connection) and privacy networks such as Tor.

The URL's or addresses, of these web sites hosted on the Tor network, are a random string of sixteen meaningless letters and numbers ranging from A to Z and 1 to 7 followed by a dot onion suffix for Version 2. Version 3 addresses are now 56 characters. Tor, or The Onion Router as you will read more about later, was developed by US Naval intelligence for military purposes and then later became open source software.[16]

These thousands of sites are enormously difficult to shut down because of the anonymity. It is the home of whistleblowers, political activists, as well as criminal activity of illegal drugs, pornography, pirated books, media, weapons, commercial hacking services, computer exploitation software, etc.

It is also the home of creative people, because they have to be creative to be able to survive there, and so innovation takes place there as well.

It is also home to security researchers looking for information that can be obtained from monitoring Dark Web communications that suggest pending malicious network intrusions.

These sites can have the high quality appearance and graphics of an Amazon, eBay, or other shopping site, but rather than using a credit card or

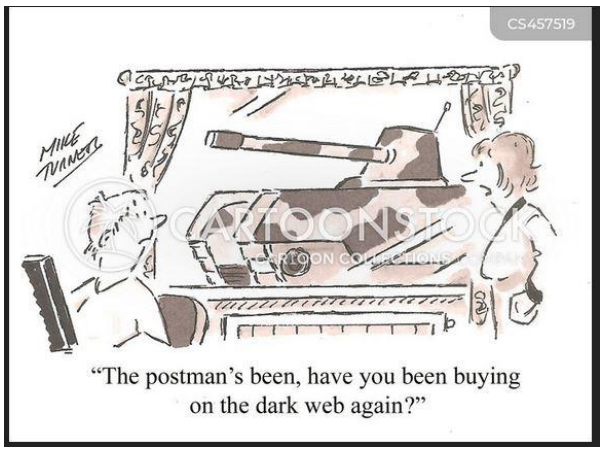
---

[16] Open-source software (OSS) is a type of computer software in which source code is released under a license where the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose.

PayPal, you pay via a crypto currency like Bitcoin.[17] The entire site is encrypted through a network of servers so that domestic and foreign intelligence mostly cannot see what you are looking at or what you buy.

These sellers of course use pseudonyms, but just like the Clear Web, as they too are governed by user reviews and value positive feedback from their customers. There is competition and choice in this world as well, with prices that routinely fall and quality that improves over time, with timely free shipping and generous return policies.

The Tor software provides anonymity by encrypting your IP address and routing the traffic through computers around the world designed to do this.



[17] *Bitcoin is a cryptocurrency, a form of digital cash.*

n0stis knew that it was now necessary, to surf the Clear Web with a virtual machine to protect yourself from the criminals and a Tor browser and a VPN[18] to protect yourself from criminals and the NSA. A VPN alone will only encrypt the message between the two end points of the VPN tunnel allowing your ISP or any other middlemen to see where you have been.

Edward Snowden speaks about surveillance and Internet freedom. The right to data privacy, is not a partisan issue, but requires a fundamental rethink of the role of the Internet in our lives — and the laws that protect it. "Your rights matter," he says, "because you never know when you're going to need them."

> "Know that every border you cross, every purchase you make, every call you dial, every cell phone tower you pass, friend you keep, article you write, website you visit, email subject line you type, and data packet your router sends, is in the hands of a system whose reach is unlimited but whose safeguards are not. " NSA whistleblower Edward Snowden's encrypted email to filmmaker Laura Poitras.

https://www.youtube.com/watch?v=0dGqR4ue8dg

As Roy Zimmerman sings in his song Hello NSA, "we are fighting freedom here at home so we don't have to fight it, over there."

If you are looking for a short version of what the Deep and Dark Webs are all about, you can read Vladimir Unterfingher's blog post and small Dark Web guide at:

https://heimdalsecurity.com/blog/how-to-get-on-the-dark-web/

The book you are reading now, will give you a basic understanding and perhaps some welcomed comic relief as well.

A more comprehensive understanding can be obtained by reading this books companion publication: A User Guide To The Dark Web (The 42nd and Final Encyclopedia Cyberspacia).

---

[18] *A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network.*

OnionShare is the solution providing the anonymity cover to the users while sharing files over the Internet in a Peer-to-Peer or P2P fashion. You might have guessed by looking at the name OnionShare; it is linked to the onion network, i.e. TOR. It uses the TOR network and allows the user to share files anonymously.

Note: OnionShare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug

https://darkweblink.com/onionshare/

Warning: Leaving your identity in the Dark Web makes it easy to trace you in the ClearWeb, monitor your actions, and by logging your IP they can show targeted advertising (based on your searches) or send malware. It is best to adopt a separate identity in the Dark Web.

ClearScore Protect, a London based Dark Web monitoring service only available in the United Kingdom, South Africa and Australia.

https://www.clearscore.com/learn/protect/dark-web-monitoring-with-clearscore-protect-for-you-for-free-forever

As famed NSA whistleblower Edward Snowden once put it: *"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."*

What is considered personal data under the EU GDPR?

The European Union's General Data Protection Regulation (GDPR) tries to strike a balance between being strong enough to give individuals clear and tangible protection while being flexible enough to allow for the legitimate interests of businesses and the public. As part of this balancing act, the GDPR goes to great lengths to define what is and is not personal data.

https://gdpr.eu/eu-gdpr-personal-data/

Chapter One, Deep Diving

Lefty felt a bit restless in retirement, and seemingly a bit older now having signed up for Social Security and Medicare. But he really did not feel old, except for reminders from his neck, back and knees hurting frequently from the ongoing and upcoming arthritis. His mind was still sharp, sharper than most his age he thought. He bristled and pushed back when he noticed that young people started treating him like some doddering old fool, by over explaining things and speaking slowly and loudly. Or being offered excessive and predatory pricing by contractors for home improvement projects.
Not to mention the relentless scam grifter phone calls about Medicare and snail mail offering hearing aids, life insurance, and cemetery services.

He understood life, perhaps better than they did. He knew what it was like to be young, but they had no idea what it was like to be old. He had pairs of shoes that were older than most of them.

To the surprise of any doctors he encountered, he did not have any drug prescriptions beyond his asthma meds and the occasional aspirin or naproxen. He did not need them and was highly suspect of them, as the television commercials became more and more aggressive in trying to sell questionable drugs to cure invented ailments to the ill-informed. Those obnoxious pharmaceutical commercials are banned in every country but the US, but should be he often fumed. It was all a bunch of proposed solutions, for nonexistent problems he believed, and with horrible side effects to boot. Restless leg syndrome, really?

His doctors eyes lit up when viewing x-rays of his knees, perhaps seeing a new car in their future, but Lefty only saw the arthritis, and the promise of the pain and suffering that lie in the future for him.

Lefty continued to maintain his four computer, three laptop, and two tablet fleet, he used for information, writing, shopping, and entertainment. He replaced the occasional failed power supply, graphics card, network card, UPS battery, or hard disk drives. These hard disks of course were typically in a RAID array[19] and imaged regularly so he never lost any data, with automated daily or weekly backup images being created as well. He applied both belt and suspenders when it came to his information on his computers. He adhered to

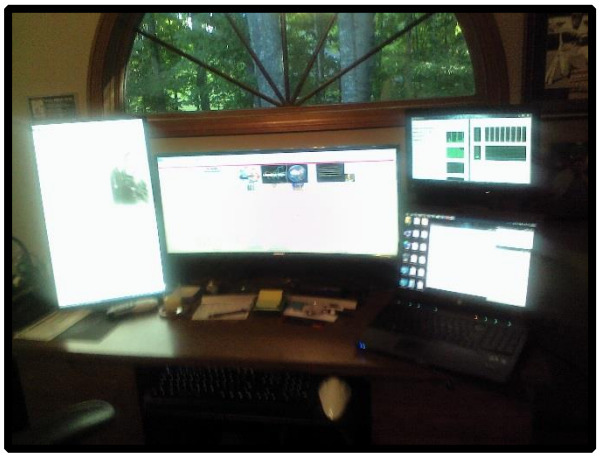
[19] RAID "redundant array of independent disks" is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both. Wikipedia.org

the old IT adage that if it is not backed up in three places, it is not backed up.

Living the rural life where few people used computers, the need for his retirement hobby of computer repair dissipated. He had donated most of his remaining computer repair and refurbishing infrastructure to a new nonprofit computer refurbisher starting up in the big city. Lefty remembered what it was like starting his nonprofit from scratch and all the people that had helped him. So he gave them most of his testing equipment, network servers and racks, benches, storage cabinets, tools, parts, and some remaining computers and peripherals. This would give them a leg up on their mission.

Little did he know he would need to hide out from a pandemic for the next few years.

Lefty so enjoyed writing stories, and did so now from his laptop writing workstation. He just could not understand how and why someone writers could do this work with a typewriter, especially without surround sound. He also enjoyed the great views of his side and back yards from his excessively windowed home in the woods while he worked.



He would occasionally see the Bald Eagles and Turkey Vultures soaring over the woods, and hear the Pileated Woodpeckers banging loudly against the trees at the back of the woods.

The creatures would come to visit out his side window to the bird feeder and below. There would be cardinals, Blue jays, goldfinches, red headed woodpeckers, morning doves (he called them chickens because they came in flocks) and other birds that he did not know the names of. Both grey and black squirrels would scamper about and attempt to get at the feeder. The occasional red fox and opossum would transverse the lawn or the woods on a hill.

The White-tailed deer came in towards dusk

The wild turkeys would visit in the afternoons

A red fox looking for mice

So now in retirement and pandemic lockdown, he had some time to go exploring into this Deep Web he had heard and read about.

Lefty setup a surplus dedicated laptop with a minimal installation of Windows 7 Pro 64-bit.[20] He installed VPN and firewall software in this installation. Once accomplished and tested, he installed a VM or virtual machine player installation of Windows 7 Pro 64-bit within that. This is where he also installed the Tor browser, firewall, and AV software.

The VM would insure that if he were hacked, that it would only disrupt the VM OS and not the host operating system. This was just another layer between him and any would be hackers.

So he booted the laptop and it automagically (automatically) established the VPN connection. He started the virtual machine and then opened the Tor browser, which opened his Dark Web search engine.

Lefty would use an onion version of a search engine to start exploring the depths of the Dark Web.

This reminded him of some thirty years earlier when he had first explored the online forums of Bulletin Boards and CompuServe with a DOS text based interface and a 2400 kbps[21] dialup modem. Now however, he had a Windows graphical based interface and a 100 Mbps[22] direct connection on a much faster and more capable computer system.

Lefty used the made up a Dark Web identity of n0stis, a Greek word (gnóstis) meaning Insider and pronounced NOSTIS. This followed the long computer science tradition of referencing Greek language and mythology and of course, the Hacker "leet" (elite or 1337) naming tradition of replacing o's with 0's. He would need this fake identify to remain anonymous as he joined the forums of hackers, criminals and regular citizens who reside there.

Note: From this point on in this book, the computer geek formerly known as Lefty has become n0stis the Dark Web explorer.

The term Gnosis[23] is not to be confused with me n0stis (or my Greek word origin gnóstis) or even my particular writing style no matter how appropriate it may seem)

---

[20] He did not use Windows 8, 10, or 11, as it is too difficult and too much repetitive work to control the built in surveillance features, and required too much diligence to maintain leakage control of them. For more details see my previous books, The Insider, and The Cozening.

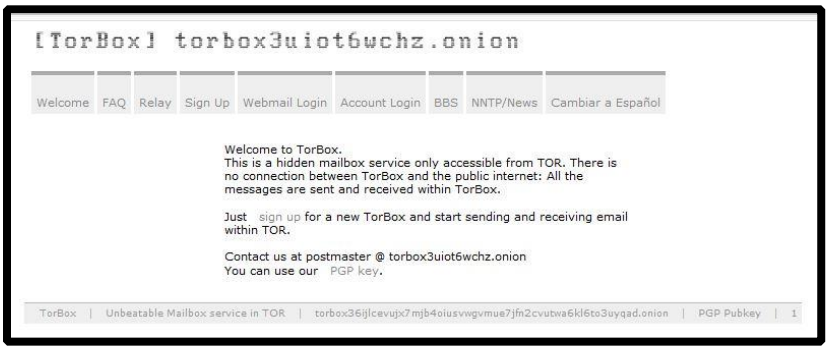
[21] 14 Kbit/s 14,000 bits per second

[22] 100 Mbit/s 100,000,000 bits per second

[23] Gnosis is a Greek noun which means "knowledge" or "awareness. Wikipedia

Note: In chaos magic, "gnosis" or "the gnostic state" refers to an altered state of consciousness in which a person's mind is focused on only one point, thought, or goal and all other thoughts are thrust out. The gnostic state is used to bypass the "filter" of the conscious mind – something thought to be necessary for working most forms of magic. (Or perhaps writing novels)

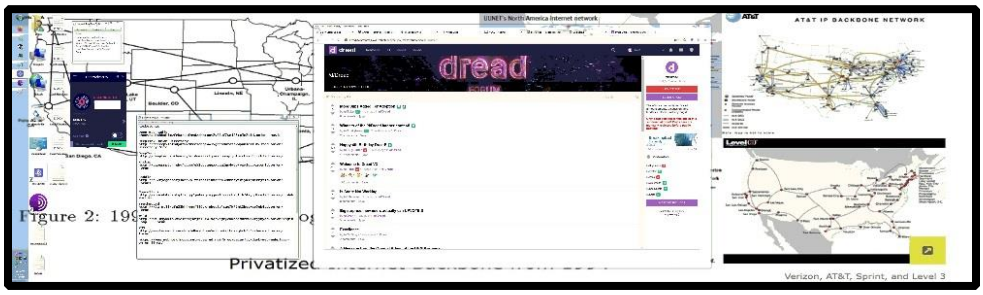
He also setup an email address in TorBox for communication, which required the use of Tor.



A few months earlier, his Deep Web research computing setup was a relatively slow Core I5 mobile processor. The overhead from the wireless Internet connection, the virtual machine, the VPN, and the Tor browser eventually made this process too slow for him. Back in the day, he used to say that he spent half his time waiting for computers and the other half waiting for women. n0stis liked speed.

So he now did his extensive research on a desktop machine, with twelve 3.4 GHz CPU cores, 64 GB memory and a 3 TB RAID mirror for storage, with a fast wireless card. He could now swivel back and forth from his writing station to his research station quite easily rather than having to slide his chair around his office.

Internet research station



Only now with a desktop configured for Dark Web research

Chapter Two, Dear Spectrum

Lefty soon discovered that the CPU, memory and network bandwidth overhead caused by the Virtual machine, the VPN and the Tor browser slowed his Internet speed to an unacceptable level for productive work like Dark Web research and writing a novel.

So he had a couple of options at this point. Elon Musk had just sent him an email to sign up to be a beta tester for his new Starlink Internet service which promised 300Mbps and a low latency or, or he could upgrade his existing 100Mbps Spectrum service to their newly offered 400Mbps service. Both were about the same monthly cost, but he would have to wait an undetermined amount time for Starlink to get enough satellites up to cover his area, and for them to build enough equipment to ship. They already had a half million preorders so this might be a problem he thought. The first shipments of the dish system, nicknamed Dishy McFlatface, would be to the northern latitudes (°N) 42.5 - 46.6. n0stis would be in that range.

Also, those who had already received it noticed a problem in northern climates. While the dish was heated (unlike DIRECTV) to prevent problems from the buildup of ice and snow, it also attracted some neighborhood friends if you did not tower or roof mount it. Of course, this was harder to do in the winter months and people tended to temporarily set the dish on the ground.

A computer chip shortage and supply chain issues did not improve his odds of getting a system either.

So the following pages will represent his experience and communications with Spectrum.

n0stis knew going into this expected ordeal that the Spectrum name represented the merger of two companies, Charter and Time Warner, both of which had the lowest “F” customer service ratings possible.

But since the current environment allows for and facilitates Internet provider monopolies with precious little consumer choice, he was pretty much stuck with this situation.

So his first step was to go online and signup for the upgrade. Not surprisingly, this is where the wheels started to come off, and spurred my first email[24] after an unsuccessful communication with their phone support. So buckle up, because here we go on a long sad adventure, which lasted several months. I was in fact their worst nightmare, a retired guy with some knowledge and a lot of time on his hands.

Dear Spectrum,

PRINT THIS EMAIL OUT, TAKE IT HOME, RELAX, CRACK A BEER, AND READ MY SAD BUT TRUE ALMOST 5000 WORD STORY. OR DOES THAT MAKE IT A SAGA?

I recently upgraded to your 400Mbps Internet service after having your mostly adequate 100mbps service for some years here. My wife and I are both retired now, and held captive in our home by the pandemic and the caravans of fools who refuse to listen to science, not wear masks, create new variants, will not take the vaccine, and may drag this virus situation out for generations, or at least for our lifetimes. My wife and I really do not like people coming into our home as we both have preexisting conditions, which make us susceptible to the virus. Although we have had the vaccine, we would rather be served by one smart technician, than three not so smart ones, who in the end accomplish nothing.

Anyway, I did not perceive a speed upgrade, I did this upgrade *online* and received no notification of when it would become active, so I called your tech support and they told me that the new speed had in fact been turned on the previous week. I explained that I was not able to discern any difference, despite the speed tests, I had done, and after arguing with them for a while, they dispatched a technician, who I will call Technician One, a few days later.

He tested cable signal strength and bandwidth with his meter and pronounced it OK. I told him that I am only getting 150-200Mbps from my Ethernet port on my router. He said that my router was _*stuck*_ and that I should replace it.

I explained that based on my thirty years' experience starting with 1200kbps dialup modems, having been an ISP, having had ISDN, DSL, TWC

---

[24] I discovered a list of names of all of their C-Suite executives and Board of Directors online and then figured out their email naming conventions so I could share my rage both frequently as well as widely.

Internet cable in two cities, and wireless broadband in two other cities that *_stuck_* was *_not_ a thing* for a router. I explained to him that this is science not magic, it is Ethernet which is a networking standard developed by Bob Metcalf et al many years ago as a grad student at MIT and engineer at the famous Xerox Palo Alto Research Center (PARC).

I persisted, also showing him that I could only get 100 Mbps on wireless with a new Win10 MS Surface Pro tablet 802.11ac connected at 5.2 GHz, so he replaced the modem with an identical modem, did not retest, and accomplished nothing. He said that there was nothing else he could do and left. Well intentioned, yet ill equipped it seems. We certainly do not want Technician One back in our home after learning of his recent vacation in Mexico during this pandemic.

I currently have four computers, three laptops, two tablets and a smart phone. They are a mix of Win7, Win10, and Android. A mix of wireless "n", "ac" and "ax" all connecting at 5.2 GHz. They all have gigabit Ethernet connections except for the phone.

I then called support again the next day to complain and argue, so they dispatched Technician Two the next week. This one was a so-called commercial installer who claims to know everything about everything. Just ask him.

He said that he had spoken with Technician One and again came at me with the *_stuck_* router thing. This must have been a concept introduced in a training session at the office, because it was assimilated wholeheartedly by this group. I told him to envision corrupted flash memory, or a bad EPROM chip as a potential problem but since there was no grease zerk on my router, I had no way to unstick it.

I questioned his testing meter, asked him to use a laptop, any laptop. He said that the company laptop he had in the van would not see 400mbps at the modem either. I asked him to explain that and he said that he did not know why and that there was nothing he could do about that. He said he could not do anything until I replaced my $300 five-year-old R7000 NETGEAR router. He said just to buy a cheap router and that I did not need an equal or better router than I had, and said the coverage would be the same to my deck and garage. It was as if his lie about the problem, if made cheaper to solve, would make me swallow it easier. I knew this to be false, because my router covered 2000 sq. ft. and the cheap ones maybe 1200-1500 sq. ft. So after speaking with NETGEAR tech support, I procured a discount and ordered this upgrade to a $350 XR1000 NETGEAR Wi-Fi 6 router covering 2500 sq. ft. so I could reach my garage and deck.

After a few days I texted him that of course the new router did not fix anything and that I had tested two additional computers of mine and got the

same bad results from the modem Ethernet port. After a series of contentious text messages that I retain but will not repeat except to say that your corporate office would not be proud of this employees conduct in person or via text. It ended with him saying that there is nothing he could do for me and me saying that he should not confuse *_can't_* with *_won't_*. Technician Two lied to me so blatantly and repeatedly to the point that I had to replace the worn out batteries in my Bullshit Detector after he left.

I complained again on yet another tech support phone call and a guy after arguing with me for a while about my insistence that my experience tells me that this is a provisioning problem, refused to connect me by phone to a network engineer. I asked him what Internet service he had and he said Spectrum 400Mbps and that he was getting 400Mbps at the router and 300Mbps on his wireless devices. I told him that I also wanted that, so he said he would dispatch a field supervisor to my home. (Multiple of your tech support people told me that this could not be a provisioning problem because the Upload speed increased from the old 10Mbps to the new 20Mbps speed.) I did then and do now believe that this is nonsense, a result of poor training and aggravated by a lack of technical and intellectual curiosity by your employees.

A phone message then informed me that I would get a service call the next week between 5-6 pm. Expecting a field supervisor, I was surprised to see Technician Three the guy who had originally installed my line many years ago. He went about solving the issue in a workman like manner, testing, and replacing the connectors and ground block in the basement and connectors at the outside box. Again, with his tester he pronounced everything OK. By running continuous randomly bad speed tests, I eventually convinced Technician Three to call a field supervisor. It was then that Field Supervisor One asked if this was an upgrade when I answered Yes, I learned that Technician Three was surprised by this. He had not been dispatched with this info and did not figure out himself that he originally installed 100mbps here and now was looking for a 400mbps connection. Anyway, Field Supervisor One quickly offered that this was a provisioning problem, as if it had happened before.

So they re-provisioned my modem and we gained a bit of speed. Prior to this, on speaker phone, I quizzed Field Supervisor One about the bad "N" Hitron modems with the Intel Puma chipset I had read about and how the Technicolor with the Broadcom chipset doesn't have these problems like DDoS, cable haunt, security problems that caused slow speeds, dropouts, and packet loss. He claimed to be unfamiliar with any of this information. I would already have this modem elsewhere in the country where 400mbps is being offered, except for this technology backwater where I live.

After the re-provisioning did not completely work and me still holding the technician hostage. I asked him to use a laptop for testing and he said that installers such as himself were not provided with company laptops. Perhaps all your installers should be equipped with an uncrippled laptop to use for *_real world_* testing.

I kept Technician Three here at my house about 2.5 hours and he was not particularly happy about that but he did try hard unlike Technician One or Technician Two. (Your phone message after all says that the service call could take between one and three hours so I was within that time line.) He also was again well intentioned but ill equipped.

After me getting him to test my wireless connection on his phone, and he got 80Mbps, Technician Three and Field Supervisor One decided that they would try to find me a Technicolor modem.

Meanwhile, beginning the next day I continued with more testing and troubleshooting connected to the Ethernet port of my router.

I then got this once and have not been able to repeat it:

So this then disproves that there is anything wrong with my equipment.

A little later in the day, I got this:

If you run this same test three times in a row and average them out, I will be around 250Mbps.

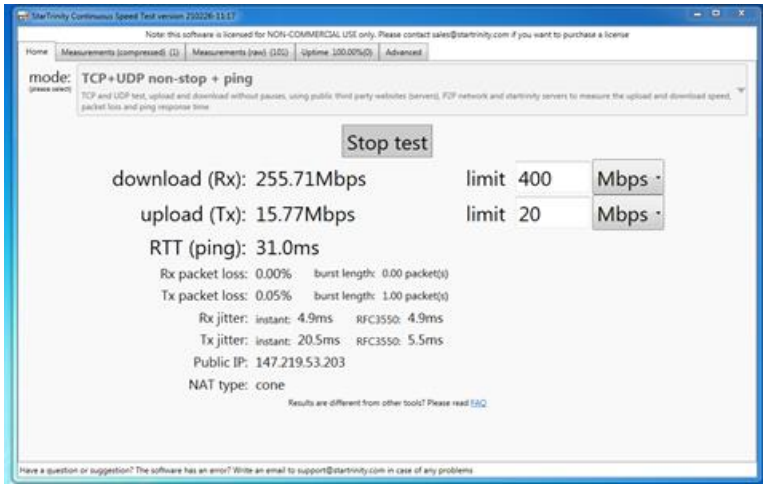
So this pretty much proves out the random nature of the 10-second tests on the speed test websites.

Compare speedtest.net, Spectrum speed test, Affinity speed test, dslreports, and fast.com sometime to see this for yourself. The test results are all over the place.

Test Site	Speed
ATT	140
Cox	158
Fast	190
Speedtest	369
Speakeasy	212
Spectrum	332
Speedcheck	128
Xfinity	156

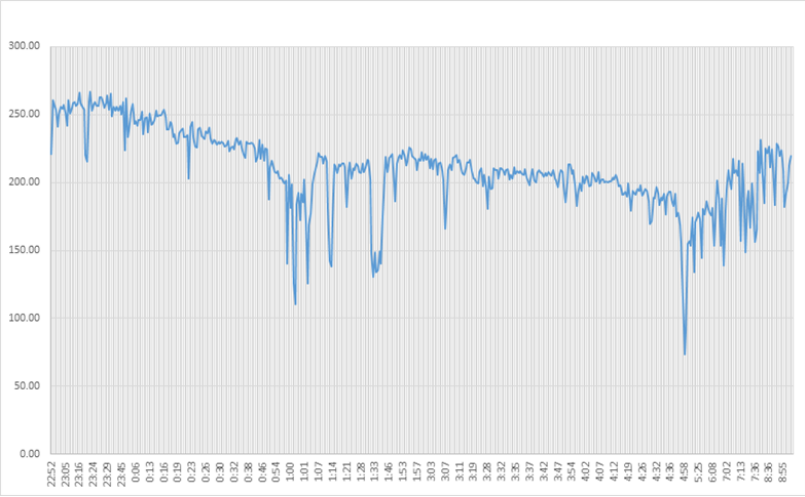
Speed tests in Mbps 8:30 am Monday

So I installed a professional continuous testing software package, did a 30-minute test, and got this:

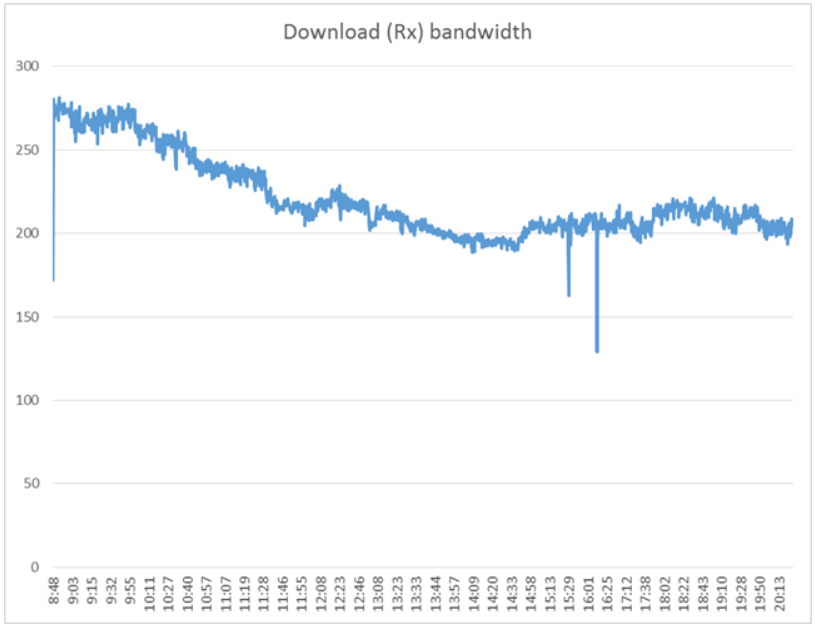


So this test points at your provisioning/equipment/ network as the problem(s).

If you still have doubts, I exported the test data to Excel, and have a look at this ten-hour evening snapshot that looks like a bad EKG or perhaps a lie detector graph.



Did some daytime testing and got this: (supporting data for these charts are available)



Called your Tech Support yesterday as I got impatient not having heard anything since last Thursday when they promised me a new modem, very soon now. Ended up speaking with one of your Customer Service Leads. He looked at the case notes, which inconveniently do not hold any reports from the three techs that have been here. He ordered a service call with a supervisor for this week.

Today shorting after receiving a recorded message from you about this visit, I get a call from a supervisor named Field Supervisor Two who says he is in the area and wants to stop in. His demeanor on the phone was immediately adversarial, not inquisitive or concerned, and certainly not appropriate for what your company has put me through this point. In a very short phone call where I agreed to his visit, he acted angry that I would not listen to the proof provided by his staff that everything was fine, despite my clear evidence to the contrary.

Field Supervisor Two arrived with this adversarial tone immediately, which can be verified by my wife who overheard the conversation. I showed him my evidence that it was not working correctly, which he dismissed out of hand. He explained that the company never anticipated so much network traffic due to the pandemic, which is overwhelming the network. This reminded me of what Technician Three had said to me early in his visit last

week that their network was at 98% of capacity. Nice! I told him I wanted to get what I was paying for and that if Spectrum could not provide it, they should stop selling it or at least stop billing for it. This would be the ethical thing to do. Half the price for half the speed would be about right, until you upgrade your network sometime in the future.

Field Supervisor Two was eventually able to find one website and one server where he could get a 400Mbps test result. But only one, and only once in a row. All other evidence points to the contrary. He persisted that the problems was in my head and not a functional problem because I was not seeing the 400 number. I had to explain number of different times that my router input speed directly affected my nine wireless devices none of which would show a speed much higher than 100Mbps individually.

I told him that he needed to stop trying to fix this problem mentally and become intellectually curious and customer focused enough to solve it physically.

Field Supervisor Two then switched tactics and gave me the whole "What do you expect me to do as I am just a lowly cable installer" routine, proving once again that the Peter Principle is alive and well at Spectrum. He mentioned that he did not understand all of this new technology as well as of his need to retire a number of times. I told him that he could escalate this up to the next level, as Customer Service had told me over the phone yesterday, and he claimed that he could not a number of times until he eventually relented and agreed that he could actually do that.

He reminded me of the Elton John song, Ground Control to Major Tom, where the lyric is "*And all this science I don't understand, it's just my job five days a week.*"

I eventually got him to replace the Hitron modem with an Ubee modem, which Technician Three had promised last Thursday, and it made no immediate discernable difference. And I eventually got Field Supervisor Two to connect his company laptop to the modem under his terms that if he got something near 400mbps he would leave my home and consider it mission accomplished. He did that and much to his confusion, he was unable to achieve half of that number. He continued to blame my equipment however, even though this had been proven wrong with three previous techs. He said that he did not want to talk about history. He also said that Spectrum never anticipated all of these people being home using their Internet connections during a pandemic. Again hinting towards network overload.

I gave him printouts of my test results to share with his counterparts in the office, and he agreed to have conversations there and perhaps escalate this case if required. The whole idea of Spectrum sending Supervisor Two here to

fix this actual problem mentally rather than physically, with an aggressive *in your face* attempted intimidation style followed by the fallback position of aw-shucks I'm just a lowly cable installer persona so feel sorry for me, was an EPIC fail for Spectrum.

Maybe we can finally **work** the problem here. I spend my whole adult life around computers and my thinking remains "Spock" like meaning logical, and scientific. I do not brook theories, speculation, and beliefs like "stuck" routers.

I am anticipating the arrival of yet another field supervisor with a Technicolor modem in his pocket and a better understanding of both his job and your data network sometime tomorrow morning.

UPDATE:

So Technician Three and Field Supervisor One showed up this morning. They did some testing, some work on the coaxial line, some more testing, replaced the Ubee modem with a Technicolor at my request, did some more testing, and became puzzled at the unchanged results.

He actually used his laptop for wireless, router, and modem testing. This is real progress!

Field Supervisor One was personable and interested in finding solutions and not assigning blame. He exhausted most of his ideas and said he would return next week to continue testing around the neighborhood with a test modem. This is the first visit by Spectrum where I was **not** frustrated and upset after it occurred. My wife and I remain **outraged** at our treatment by Field Supervisor Two during yesterday's visit and Technician Two's visit previously.

Field Supervisor One was kind enough to provide me with his email address so I shared with him the data that created the charts shown above. I also shared yet another alternate idea for testing download speed, by *actually* downloading files. It did shock me however to learn that the same guy who claimed to have looked at the overall network bandwidth utilization for the past several months and said it was OK, and also looked at the modems of my neighbors in this subdivision, but then claimed he did not know if any of the other 25 or so homes here were provisioned for 400Mbps or 1000Mbps service. This to me would be a key piece of information, but what do I know.

At least now after five visits by five technicians, over what is approaching one month and again in the midst of a pandemic, we have finally graduated from the:

1. The initial it's the customer's computer
2. To it's the customers router
3. To it's the customers home wiring
4. To it's the wiring at the PED

5. To it's the servers on the testing websites
6. To it's the testing software the customer is using
7. To it's ***our*** network that is the problem, I guess we had better test that now.

This is progress. To be continued…

So I am waiting to hear back from Field Supervisor One on his local network testing results:

In the meanwhile, I have discovered that a network traceroute shows 17 hops[25] (routers) for me to get to my Internet provider Spectrum.com and 13 hops to my email provider.

Today I replaced the existing Ethernet Category 5e (1Gbps) cables from my router to your modem, and from my computer to my NETGEAR RX1000 router with Ethernet Category 7 cables (100Gbps). I did this not because I am expecting or need 100Gbps bandwidth from Spectrum, (I would settle for 1Gbps symmetrical) but because of the exceptional electrical shielding on these cables that will eliminate any chance of existing electrical interference. I just want the 400Mbps you charge me for and not the 200Mbps or so you are currently giving me. I found no discernable difference in speed with these new cables.

But really? From 1200kbps to 940Mbps over 35 years? Hell, there is at least 20 years of telecoms promising fiber optic cable in there. All of you in the telecommunications industries, should be ashamed of yourselves, if that is the best you can do. As if that is what the country that invented the Internet deserves. Kids seeking an education are shut out because they live too far into the country or too deep into the cities and there is just not enough money to be made there for you despite the government corporate welfare you receive.

Professionals trying to work in this pandemic have to put up with stuttering video calls, even live on national TV. You should shutter every time you see this. And yes, feel ashamed. And especially for the dropped connections for the kids struggling to learn. But I digress…

I am starting to question your network architecture after this testing:

Warning: Clear Web sites.

---

[25] A traceroute will show you how many layer 3 hops you are getting through from A to B. However you could be going through hundreds of switches in between. You could also be going through 10 ISP routers running a layer 2 VPN which appears as a single hop. An MPLS network could hide its internals, or show its internals to you. You could have transparent firewalls in the path as well.

Set by speedtest.net as optimal (closest)			
Renaissance Learning, Inc. Wisconsin Rapids, WI	*https://www.renaissance.com/*	*153mbps*	*18 hops*
Preferred by Spectrum techs			
Nsight Green Bay, WI	*https://nsight.com/*	*231mbps*	*18 hops*
CyberLynk Network Milwaukee, WI	*https://cyberlynk.net/*	*319mbps*	*13 hops*
Ethoplex, LLC Milwaukee, WI	*https://www.ethoplex.com/*	*273mbps*	*12 hops*
•Always six hops through Charter routers *•Less hops appear to equal higher speed test bandwidth*			

So as it turns out, me getting Field Supervisor One to give me his email address was a pyrrhic victory because he is unresponsive to my emails.

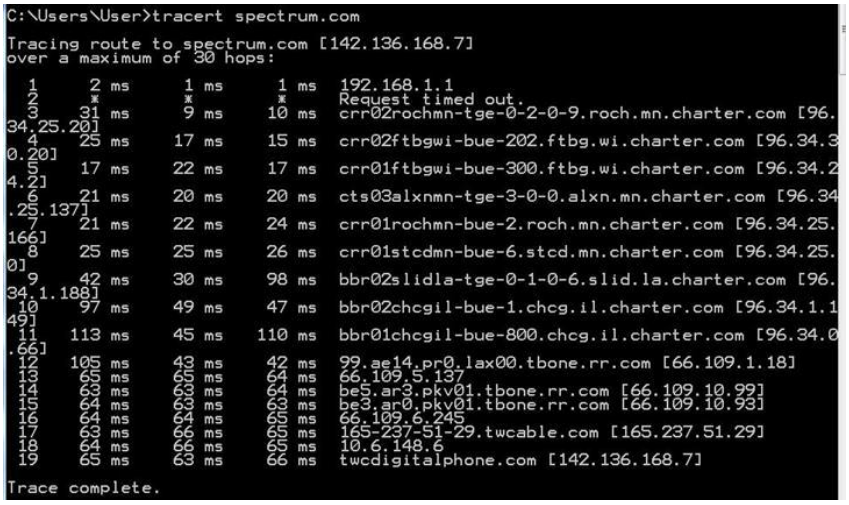
This whole experience has apparently brought out my inner B.B.King blues. So I wrote you this song.

Spectrum Blues
With six or more hops to anywhere
Spectrum is getting me nowhere
I want to go to Amazon to buy underwear
But I need to take six hops just to get there
Chorus: My traceroute leaves no doubt
And it makes me want to shout
Your six hops to anywhere are bringing me down
I need nine hops to get to Google

Try to get that into your noodle
When it takes six hops to the bank to get my money
I am not thinking that gee this is sure funny
Chorus: My traceroute leaves no doubt
And it makes me want to shout
Your six hops to anywhere are bringing me down
In this pandemic where stupidity seems to be endemic
Nine hops to order groceries only feed the epidemic
Spectrum won't give the speed that they promise
So I've come to realize that they have led me amiss
Chorus: My traceroute leaves no doubt
And it makes me want to shout
Your six hops to anywhere are bringing me down
And unlike the six degrees of Kevin Bacon
With six hops to anywhere, it's not speed that I am take' in
LiMu Emu and Doug say to pay for only what I need
But after paying Spectrum more, I can't even get their promised speed
Chorus: My traceroute leaves no doubt
And it makes me want to shout
Your six hops to anywhere are bringing me down
Five of their technicians seem clueless to you
They all say there is nothing they can do
I guess it could be said if you pay Spectrum
You are going to end up getting it in the rectum
Chorus: My traceroute leaves no doubt
And it makes me want to shout
Your six hops to anywhere are bringing me down

Back in the late 80's when I started connecting to the Internet you judged an ISP by how many hops to the POP, or Point of Presence. (Internet Backbone) This was especially important with dial-up connections. In the trace route I have run you can see my packets ping ponging around your network about 19 times before hitting home. I do not know if this is a result of your merger, I do not know for sure that it is part of my problems, since I am not a network engineer, but I think that you really could stand to clean up your shit here.

I can understand me hitting your local router, your Eau Claire router, (where your speed test server is) but then it should hit the Chicago or Minneapolis POP real soon after in my mind. Of course, again I am not a network engineer, just a lifelong computer geek and an unhappy customer.



```
C:\Users\User>tracert spectrum.com

Tracing route to spectrum.com [142.136.168.7]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3    31 ms     9 ms    10 ms  crr02rochmn-tge-0-2-0-9.roch.mn.charter.com [96.
34.25.20]
  4    25 ms    17 ms    15 ms  crr02ftbgwi-bue-202.ftbg.wi.charter.com [96.34.3
0.20]
  5    17 ms    22 ms    17 ms  crr01ftbgwi-bue-300.ftbg.wi.charter.com [96.34.2
4.2]
  6    21 ms    20 ms    20 ms  cts03alxnmn-tge-3-0-0.alxn.mn.charter.com [96.34
.25.137]
  7    21 ms    22 ms    24 ms  crr01rochmn-bue-2.roch.mn.charter.com [96.34.25.
166]
  8    25 ms    25 ms    26 ms  crr01stcdmn-bue-6.stcd.mn.charter.com [96.34.25.
0]
  9    42 ms    30 ms    98 ms  bbr02slidla-tge-0-1-0-6.slid.la.charter.com [96.
34.1.188]
 10    97 ms    49 ms    47 ms  bbr02chcgil-bue-1.chcg.il.charter.com [96.34.1.1
49]
 11   113 ms    45 ms   110 ms  bbr01chcgil-bue-800.chcg.il.charter.com [96.34.0
.66]
 12   105 ms    43 ms    42 ms  99.ae14.pr0.lax00.tbone.rr.com [66.109.1.18]
 13    65 ms    65 ms    64 ms  66.109.5.137
 14    63 ms    63 ms    64 ms  be5.ar3.pkv01.tbone.rr.com [66.109.10.99]
 15    64 ms    63 ms    63 ms  be3.ar0.pkv01.tbone.rr.com [66.109.10.93]
 16    64 ms    64 ms    65 ms  66.109.6.245
 17    63 ms    66 ms    65 ms  165-237-51-29.twcable.com [165.237.51.29]
 18    64 ms    66 ms    65 ms  10.6.148.6
 19    65 ms    63 ms    66 ms  twcdigitalphone.com [142.136.168.7]

Trace complete.
```

I have had no contact with or communication from Spectrum in more than a week now, leading me to believe that they have now just blown me off. So maybe it is over.

Well, after five consecutive days with me reporting my various test results, the last of which acknowledged my blues and included the lyrics above… I got a phone call from Field Sup One.

He said he had done some testing in my neighborhood earlier in the week at a few of my neighbors and had the same poor test results that I experience. I asked him again if anyone else in my subdivision could get a higher speed and he lied, I later discovered, and told me, that was a Billing thing and he did not have access to that database. He said that his meter reads fine and when I suggested that the meter might be the problem he scoffed at the idea. Instead, he is going to order yet another test modem and perhaps a different laptop to do more testing next week. He said the system tested good at the office fiber outlet, so I asked if he tested at the junction where the fiber terminated and the coax cable started in my area and he apparently lied again and said that he did not know where that node was. Really? How many months will it take to get this escalated to your engineers?

It seems to me that your plan here is to find the right combination of modems and computers to fix this mentally with me, rather than trying to fix it physically. I am now fully and completely fed up.

In A World Of "Some Setting Of Contents Will Occur During Shipment, Batteries Not Included, Objects In The Mirrors May Be Closer Than They Appear, We Have The Right To Change These Terms And Conditions Without Notification". We Now Get From Spectrum "We Only Guarantee 70% Of He

Speed You Are Paying For.“ And You Can’t Even Meet That Low Bar.” Last time I Checked, 70% is a C- in school.

I have discovered in going through **all of this** what the majority of your staff is **not**, and that is intellectually curious. Not just about their job duties but about related things like routers, modems, and computers. This is a missing ingredient for quality service, in my view.

One of the keys to my success in creating and running two IT related businesses over thirty years was a strong curiosity and interest about all things computer and telecommunications. The pace of change and complexity in this business over these past 30 years requires this attribute to even want to do it, much less be any good at it. This embedded interest continues today into my retirement and is also a key to many others in tech like Bill Gates and Elon Musk.

So all of this started with me taking a chance on a Spectrum upgrade to improve my speed rather than getting a Starlink satellite dish from Elon. This situation has cost me countless time and frustration as well as the cost of a new router. All of this for a retired guy on a fixed income, with too much time on his hands apparently.

I do not really know how much of all of this can be blamed on ignorance/incompetence and how much on malfeasance/skullduggery but I suspect that a big portion of each is involved. Keep in mind that I would already have 200mbps service like the rest of the country, except your monopoly allows you only do this when you have to compete with AT&T fiber.

Remember, you started this by taking my money and lying to me by blaming my equipment, and it is still not fixed a month later. This should be a cringe-worthy technical support and management horror story for anyone reading it.

PS. I just cannot wait to talk to your billing people and try to get them to not continue to charge me for what I still do not have.

I know you probably don’t care, but try to Imagine if you can, two really badly rated corporations who merge and change their name (as a disguise) but who then to the surprise of everyone seek to redeem themselves in the eyes of the general public by spurring economic development in rural areas by providing a service that boosts educational and employment opportunities for its human capital. They then choose this task as their raison d'etre and as their primary goal superseding the previous well-worn maximizing shareholder value mantra. They come to understand that you can do well, and do some good at the same time. Just Imagine it.

Dear, Dear, Spectrum, the sequel

(Or another 4000 words)

The scene begins at Charter Communications, Inc. Headquarters[26]

Then cut to a CHARTER corporate office boardroom.

As the scene unfolds, a VP in Corporate Marketing is walking into a hastily called meeting where the attendees are jamming to the Got the Spectrum Blues song with its BB King like guitar riffs and the Chuck Berry like honky-tonk piano licks blasting over the PA system. He cuts off the speakers and then addresses his staff, as well as a small customer support contingent.

Folks, he says, "When our customers are sending us blues songs that rhyme our trademark name Spectrum, to their experience with us of *getting it in the rectum*, we may have a corporate image problem. What do you all think?"

---

[26] *Charter Communications, Inc./Spectrum - Mission Statement To integrate the highest quality service with superior entertainment and communications products that consistently exceed the expectations of its growing customer base.*

https://mission-statement.com/spectrum-mission/

The sound in the room is nothing but crickets for an uncomfortable period until finally the new guy in customer support shyly speaks up. "*I have an idea, what if we were to upgrade our systems to be able to deliver what we promise? We could actually deliver a service commensurate to what our customers are paying for, what they expect, and want. They could eventually learn to love us. By doing this, we could actually fully embrace our Mission Statement. Let's show everyone that we are part of the good 50% of employees.*"[27]

There are another few moments of stone silence, followed by the whole room breaking out into raucous laughter. After several minutes of this, the VP finally breaks into the ruckus still laughing, "*We _could_ do that… but NAAAH!"*

Early the next Monday morning I received a phone call from a personable gal, a corporate escalation specialist she said, informing me that I would be receiving another call within 24 hours from yet another person to work on my problem. Because of my most recent email, her job she said was to direct my email to the proper person(s). She questioned me about her concern over proper COVID protocols being followed by local technicians. I explained that she had misunderstood my mention of a local technician who had vacationed in Mexico in my email. I said that it was not because he came to my house after vacation, (he came before this), but my point in my original email was that I did not what that tech back in my house for at least two weeks afterwards. Since Field Supervisors are always accompanied by a tech (per Bob over the phone with corporate) I wanted to make sure that he did not show up at my house. I asked if she had read my rather lengthy email and said that she had enjoyed my song lyrics but had not listened to the attached song. I told her she should because it was a song about unrequited love and was most certainly worth a chuckle.

Later that day, the avalanche of fecal gravity I had apparently triggered by my email to Charter corporate (or perhaps it was my song lyric rhyming Spectrum with rectum) began to flow. Anyway, this downhill flow had now achieved sufficient velocity so that late in the day I received a call from a nice guy who he said was the manager of Field Supervision for Eastern Wis. He called me from your southeastern office, and was following up. He said that this was based on a request from corporate and indicated that he would dig into my issue with the local office and would get back to me RSN. He also said that he had two main goals. The first was to solve my problem and the second

---

[27] *Charter Communications, Inc.'s mission, vision, & values motivate 50% of employees. Comparably data clearly shows that a focused mission statement and cohesive core company values are vital to maintaining employee alignment.*

https://www.comparably.com/companies/charter-communications-in/mission

was to find out what kind of screw-ups had caused this problem to end up on his desk. I think he was a bit annoyed that a VP had kicked this problem into his Inbox. I asked him if he had read my email, and he said he had not yet seen it. Really? He never did get back to me, but sent someone else instead.

The next day late in the day. I received a call from Field Sup. Mgr. One who he said is in charge of the local Field Supervisors, and Field Supervisor One's boss. (This is number six technician if you are counting, as I am.) He said that he was in my neighborhood today with a tech doing some testing and had positive results to report. I questioned him about how his testing differed from the bad tests that Field Sup. One had reported to me last week. He said that he had not spoken with Field Sup. One because as you know he works Wed. to Sat.

Note: How the hell would I know that? I am not and do not want to be involved in managing your company much less your personnel schedules. Although I think, I have learned your management structure over the past five weeks, because I have met or spoken with all of them. If pressed, I could easily whip up a local Spectrum org chart. My job as I see it, as an unsatisfied paying customer is only to point out the flaws and deficiencies in your business service delivery as I see them.

I then pressed Field Sup. Mgr. more about the testing, and he said he was using a modem provisioned for 600Mbps and his phone and laptop. He said that he really did not trust the laptop because it was so loaded with corporate software overhead (vpn, encryption etc.) that it would skew the results. I asked him if he had tested where the fiber changed over to coaxial/copper and how far away from this subdivision that was. He said no and that he did not know. This Again! Really? One of the many key things that I have learned over my thirty years in the IT business is that consistency of test methodology logic is important. Randomly switching out modems and laptops until you get the desired results is a bit of a shotgun approach and appears to me to be doomed to failure.

Note: Is it not possible to give your techs the tools they need to do their jobs? A meter and a phone are not the proper testing tools when most people are connecting computers to your network. It may seem silly, but how about you actually give them an Ethernet/wireless laptop that they can use for testing? **Ideally, it would not be used for anything else but this. You do not have to call it a laptop, you can call it a** meter i**f you like.**

I also shared with Field Sup. Mgr. One some info including my own testing which I had previously reported via email to Field Sup. One a day earlier. This was news to him, because of course he had not spoken with Field Sup. One yet. Apparently, your business has not yet discovered email as a valuable communication tool. God forbid you would use twenty-year-old database technology for the techs to enter in case notes, and share that across the corporation with something like SharePoint. He said that he ran out of time today, but would return tomorrow accompanied by Field Supervisor One to do more testing at my PED and *speak with me personally.*

Note. Oh, Oh, does this mean more trying to fix this mentally with me will be in play? Or does it mean that I am going to get a modem provisioned at 600mbps to be able to get my provisioned 400Mbps? Stay tuned for the next episode…

The next day, Field Supervisor Mgr. One and Field Supervisor Three showed up around midday. That is technician six and seven now if you are still counting. Mostly it was the first option from above, but by nicer guys at a higher level of competence and intelligence. They spent about half hour tapped into my PED to some equipment in the van and made some phone calls. **In the three hours or so that they were here in the house, the speeds got progressively better, but only at speedtest.net.** I suggested using a scientific method of testing three sites and averaging them out, but that did not fly with them. I did notice on a trace route test, that Charter redirects from speedtest.net to their own server and Field Supervisor Mgr. One readily owned up to that fact. There were also wide variations on speed depending on if you use IE, Edge, Chrome, Firefox, or Pale Moon browsers. I did not see a scientifically sound testing program in use here, and it led me to think that I do not understand all I know about this.

For example, my Surface Pro tablet had been doing about 100-150mbps on wireless and was doing 300mbps by the time they left. This is with no changes to the router or the tablet. Go figure. This evening, I cannot repeat those results.

On my one Ethernet, connected computer Field Supervisor Three reset the Ethernet card in my computer speed from 1 GB full duplex to auto and back and claimed some improvement from that. After they left, I could no longer achieve the same speeds either wired or wireless.

I think that a couple of things happened here. First, they did some provisioning tweaking of my connection from the van, which did not take immediate effect, as the modem was disconnected and turned off for the

testing. I think some evidence for this idea is that my upload speed seems to have moved from a consistent 20mbps or less, to a consistent 22-23mbps. Second; bombarding your speedtest.net server repeatedly perhaps did some kind of temporary data caching and improved the test results.

I do not want to seem like a cynic, but my CST continuous speed tester software still shows my speed at or below 250mbps, and all the other nine speed test sites show results well below my provisioned 450mbps on an Ethernet connection.

My five wireless "n" machines (300mbps Max) continue to get 60-100mbps. On one of these, I got 150mbps last week and only 60mbps today.

My three wireless "ac" (600mbps Max) machines continue to get 150-250mbps.

The next day I left a voicemail for Field Sup. Mgr. One making a request to try their 700Mbps test modem here. Field Sup. Mgr. One called me back today; he is coming tomorrow with the test modem they have been using for final testing here.

Meanwhile (I had some time to kill) so I searched the Spectrum page on the web to see if I could notice any mandatory disclaimers resulting from your loss in recent litigations, $60 million FCC fine, and government forced marketing changes in NY state, and all I found was this:

Go Faster with Spectrum Internet® Ultra

- Choose Internet Ultra for speeds starting at 400 Mbps (wireless speeds may vary)
- Enjoy a faster download speed, more consistently than any other provider.††

††Based on the latest FCC Broadband Report (in tiny print at the bottom of the page)

A little further research revealed that this report was generated from the broadband providers own self-reporting to the FCC, and interestingly enough a search the 50 page pdf of this 2020 report and appendices for the keywords of Charter or Spectrum came up empty. I also found no comparisons of speed or anything else in the report with any other company. Go figure!

I did find this in an appendix however:
2020 FCC Report Appendix (again, self-reported)

State	10/1 Mbps	25/3 Mbps	50/5 Mbps	100/10 Mbps	250/25 Mbps
Wisconsin	67.3%	56.1%	51.1%	48.2%	1.4%

So I appear to be trying to join the 1% club!

A few days later, Field Sup. Mgr. One arrived with the test modem around midday. On speedtest.net, the new Ubee modem delivered 600Mbps down and 40Mbps up to his Dell laptop using Chrome, either wired or "ac" wireless. It delivered less using IE. It delivered the same also Ethernet and wireless on his smartphone, again using Chrome. It delivered 400 plus Mbps consistently to my Ethernet computer, 125Mbps wireless "n" to the same computer two feet away from the NETGEAR XR1000 router. It delivered approx. 150-250Mbps to my wireless "ac" computers and 50-100Mbps to my wireless "n" computers all tests using a 5.2GHz connection. Use of Firefox, IE, or Pale Moon did not seem to impact the performance.

Switching back to the Technicolor 400Mbps modem brought back the inconsistent speed tests ranging from 350-450Mbps tests, and a max of 200Mbps to a wireless "ac" tablet. During all of these tests, the CST software reported a max of 250Mbps.I would call this *Internet speed* versus *Charter speed*.

I again asked if anyone else in my area had speed above 100mbps, and how far away the fiber ended and their copper started. They said, they do not know, to both of these questions repeatedly which means you are not willing to share this information apparently.

I do not hold Spectrum responsible for the networks outside of their own, but testing speed at **one** website redirected to your own network repeatedly cannot really be seen as indicative of a customer's experience on the Internet. Even then, the test results are not consistent and repeatable to your own redirected speedtest.net site. When still on your network, test results at https://www.spectrum.com/Internet/speed-test are about half of that (200mbps) but also inconsistent and can range up to 350mbps.

My takeaways both from today this whole Spectrum saga to this point are these:

1. If you have the patience and persistence to stay after Spectrum and hold their feet to the fire, they eventually will and can make it better. It does not hurt if you are retired with some time on your hands and

locked in your home due to a pandemic. After all, I went from a consistent 150mbps Ethernet to a consistent 300mbps on my original test computer on Spectrums network.

2. Apparently, if you do not have a specific Spectrum Dell laptop with a Chrome browser and wireless "ac" you will not get consistent speed tests. Remember, three other technician Spectrum HP laptops could not achieve the speed at my house or at neighborhood PED's)
3. Apparently, if you don't have a Spectrum smartphone with an OctaCore (dual quad core) processors and 10Gb Ram you will not get consistent speed tests (my wife's two smartphones will not crack 100mbps)
4. OS and network hardware are more important beyond 100Mbps. If you have Win7 and "n" wireless, or Win7 and gigabit Ethernet, you will not get there consistently. If you have Win7 and "ac" wireless, you will not get there either. My six month old Surface Pro tablet with Win10 and "ac" wireless you will not get there either with Firefox or Edge.
5. Firewalls, browser extensions, and antivirus software are not significant factors in bandwidth testing.
6. Browser software like IE, Firefox, Edge, and Pale Moon will not give you consistent Spectrum speed tests
7. Spectrum will not put 1GB files on one of their network servers for download testing, because they cannot maintain 400Mbps for more than 10 seconds at a time
8. 400mbps of Charter speed is actually about 250Mbps or less of actual Internet speed as determined by CST and overall user impressions
9. Spectrum appears to have these same problems with their 600Mbps-40Mbps (commercial) and 940Mbps-40Mbps (residential) copper deployments
10. Symmetrical 1gb fiber deployment is our only hope in the US as we currently rank 12th in the world in broadband speed availability

I am reluctant to revisit the whole hops thing, as I pretty well beat this horse to death in my last email and song. But these traceroute results just appear to me to be a bit schizophrenic. Excessively ping ponging around, via your peering agreements apparently, to get to the POP backbone. I have no malicious or nefarious intent here, am just trying to understand this. There are many routers involved here and latency can exceed 250ms in the later hops. Since traceroute measures the time it takes to get each response it has no way of knowing if any delays were encountered on the way out to the destination or

on the way back, potentially providing misleading results.

My conclusion is that the Spectrum network will not consistently deliver 400Mbps to me even on your own network, but it is an *upgrade* from my previous 100Mbps service. Customers like me must decide if half of a promise is worth an extra twenty bucks a month on an already overpriced noncompetitive service.

While I will not concede that your service meets my expectations, I will concede now that my results here are as good as you can currently make it.

Intro: My Dear, Dear Spectrum, does our unrequited love affair need to continue, or will you love me tomorrow?

Let us slow my roll now, like my Internet, with another love song from me to you.

Got The Fiber Blues

I wrote you a letter and expected to hear crickets
Cause my Internet packets still act like they have rickets
With phone calls you responded and technicians you did dispatch
They did their best but all they could do was make a patch
Chorus: My packets ping pong around your routers
Slowing me down and making me a doubter
Your monopoly behavior is telling
But it's not to me you will be selling
The millennials may use it for their mobile phone
But I want some real speed to come to my home
Chorus: My packets ping pong around your routers
Slowing me down and making me a doubter
Your kind has promised fiber for thirty years
Yet your network of band aids are leaving me in tears
We all want a network of fiberglass
Yet the copper you give me is just a pain in the ass
Chorus: My packets ping pong around your routers
Slowing me down and making me a doubter
Your mergers make you all more money
But to those of us who suffer, this is not very funny
Discount and freeze the cost if you want to be a suitor
Till you can get some overdue fiber to my computer
Chorus: My packets ping pong around your routers
Slowing me down and making me a doubter

I will grant you that network upgrading is a bit of a chicken and egg thing. On the other hand, if you build it they will come. The 11 countries ahead of us on bandwidth must know something we do not or that we willfully ignore in this country.

Predictions can be difficult.

> *IBM introduces the PC and, with Microsoft, releases DOS ("640K ought to be enough for anyone"* — Bill Gates 1981)
>
> https://quoteinvestigator.com/-2011/09/08/640k-enough/

> *"Residential services will depend on high-speed Internet access. High-speed today is 100 Kbps to 900 Kbps. This will increase in the future to 1 Mbps to10 Mbps for each household."*
>
> https://www.pearsonhighered.com/assets/-samplechapter/0/1/3/0/0130281360.pdf

"We don't like their sound, and guitar music is on the way out." — Decca Recording Co. rejecting the Beatles, 1962.

https://quoteinvestigator.com/2013/04/27/guitars-out/

So on my own personal computers, memory has increased from 640k to 64 gigabytes in approx. 25 years. About a 10,000% increase.

My promised telecommunications speed has gone from 1200kbps to 400mbps in approx. 35 years. About 3000% increase.

Here is what your competition would be like if we actually had a free and open market, you know what I mean here, that whole invisible hand of the free market thing that conservative businessmen like to talk endlessly about.

- Charter/Spectrum 400 Mbps/20 Mbps $69.99/$94.99.
- 940 Mbps/40 Mbps $89.99/$114.99
- Verizon FiOS Gigabit Connection provides 940/880 Mbps speeds for $69.99 /mo.
- AT&T Internet 1000 940/880Mbps $60 /mo.
- Gigabit Internet by XFINITY from Comcast 1 Gbps/35 Mbps $70.00 /mo.
- Gigabit Pro by XFINITY: 2Gbps/2Gbps (Fiber To The Home / FTTH) **OMG!**

In the end, it seems to me that Charter/Spectrum would benefit from Cranium-Rectal inversion therapy to be able to fully grasp the need to build a fully fiber optic gigabit symmetric network into the homes of your customers. Once this procedure is complete, you may just discover that worshiping at the altar of Wall Street is in fact a death cult, and that we humans do in fact have a higher purpose than to be coin-operated, terrestrial, bipedal, carbon based lifeforms.

PS. Hey Charter, one of your tone deaf and clueless competitors just threw in the towel. See below. Here is your chance! And it looks like there is another Federal corporate welfare program coming to you in the new infrastructure bill. Now your response is that you want to have data caps put in place as a condition of your merger. You are deploying asymmetric 1gbps fiber in some locations. 940mbps down and 40 Mbps up? Really?

AT&T Lobbies Against Nationwide Fiber, Says 10Mbps Uploads Are Good Enough (arstechnica.com) 192

Posted by BeauHD on Monday March 29, 2021 @08:01PM from the don't-fight-it-embrace-it dept.

AT&T is lobbying against proposals to subsidize fiber-to-the-home deployment across the U.S., arguing that rural people do not need fiber and should be satisfied with Internet service that provides only 10Mbps upload speeds. Ars Technica reports: AT&T Executive VP Joan Marsh detailed the company's stance Friday in a blog post titled "Defining Broadband For the 21st Century." AT&T's preferred definition of 21st-century broadband could be met with wireless technology or AT&T's VDSL, a 14-year-old system that brings fiber to neighborhoods but uses copper telephone wires for the final connections into each home.

"There would be significant additional cost to deploy fiber to virtually every home and small business in the country, when at present there is no compelling evidence that those expenditures are justified over the service quality of a 50/10 or 100/20Mbps product," AT&T wrote. (That would be 50Mbps download speeds with 10Mbps upload speeds or 100Mbps downloads with 20Mbps uploads.) AT&T said that "overbuilding" areas that already have acceptable speeds "would needlessly devalue private investment and waste broadband-directed dollars." "Overbuilding" is what the broadband industry calls one ISP building in an area already served by another ISP, whereas Internet users desperate for cheaper, faster, and more reliable service call that "broadband competition."

PPS. Here is yet another example of the kind of wrong-headed thinking going on these days:

ISP Imposes Data Cap, Explains It To Users With Condescending Pizza Analogy (arstechnica.com) 85

Posted by BeauHD on Friday April 02, 2021 @06:00PM from the poorly-thought-out-illustrations dept.

An anonymous reader quotes a report from Ars Technica:

Cable company WideOpenWest (which markets itself as WOW!) yesterday told customers that it is imposing a data cap and explained the change with a pizza analogy that would seem more appropriate for a kindergarten classroom than for an email informing Internet users of new, artificial limits on their data usage. The email said WOW is "introducing a monthly data usage plan for your Internet service on June 1, 2021" and described the system as follows:

"What's a monthly data usage plan? Let us illustrate ... Imagine that the WOW! Network is a pizza. Piping hot. Toppings galore. Every WOW! Customer gets their own slice of pizza, but the size of their slice is dependent on their Internet service plan. While customers who subscribe to 1 Gig get the largest slices, those with Internet 500 get a slightly smaller piece, and so on. But, it is all the same delicious, high-speed pizza that you know and love. Now, say you are not full after your slice and you grab another. That extra slice is like a data overage. Do not worry -- we got extra pizza... umm, data... just in case. If you exceed your data allowance, we will automatically apply increments of 50GB for $10 to your account for the remainder of the current calendar month. Total overage charges will not exceed $50 per billing statement no matter how much data you use. Even better -- the first time you experience a data overage, we'll proactively waive fees."

The email did not mention that, unlike pizza, Internet data does not run out and that there is plenty for everyone as long as a network is properly constructed and provisioned. And despite paragraphs of comparing data to pizza, the email literally never says how much data customers will be allowed to use before they are charged extra. The answer is in a newly updated "network management practices" document that says the monthly cap will range from 1TB to 3TB: the 50Mbps download plan gets 1TB, plans between 100 and 300Mbps download speeds get 1.5TB, the 500 and 600Mbps plans get 2.5TB, and the gigabit plan gets 3TB.

WOW has over 800,000 Internet customers in parts of Alabama, Florida, Georgia, Illinois, Indiana, Michigan, Ohio, South Carolina, and Tennessee. In a separate document, WOW says that "unlimited data plans may be added for an additional monthly charge" but does not say how much it will cost.

It is apparently not a bad April Fools' Day joke, either. People in the DSLReports forum have reportedly confirmed the changes with a WOW representative.

Reference

Telecom Book of Broken Promises.pdf http://teletruth.org/

"We are in the middle of a pandemic. So much of modern life has migrated online. As a result, it has become painfully clear there are too many people in the United States who lack access to broadband. In fact, if this crisis has revealed anything, it is the hard truth that the digital divide is very real and very big"

https://docs.fcc.gov/public/attachments/FCC-21-18A3.pdf

Dear, Dear, Dear Spectrum

(Now a Trilogy with another 3000 words)

What has been missing here so far in this saga is for you to add some insult to injury. Well, it came in the mail today and it was only a matter of time. So you billed me for the extra twenty bucks for an upgraded monthly service, I am not able to achieve for the past six weeks, but you have been working on it, or at least pretending to. This is in itself bad enough, but you have the combination of ignorance, incompetence, and malevolence to now add an additional charge of $50 for a service call. This is salt in the wound and has further provoked me, yet again.

So once again provoked by your company, I spoke with a nice gal in billing who could not figure out a way to deal with this issue and so she transferred me to her manager, who turned out to be a real ass. This is a great personality attribute for a Customer Service Mgr.

He was insistent that since the first two techs indicated that the problem was my equipment so the charge was applied even though I was not notified by phone support that I might incur this charge when I asked him to dispatch a tech. He said that this was not a requirement by policy.

Keep in mind that your first tech was well intentioned but ill equipped to solve the problem, your second tech was a sarcastic abusive bull shitter who readily admitted that his own laptop would not achieve the rated speed, but pronounced my original router, and all eight of MY computers bad, and your system OK based on his phone connected to MY wireless router.

There is a lot of talking out of both sides your mouth here, by saying that the router is MY equipment that they are not responsible for, while at the same time pronouncing your system OK, based on one of your phones connected of course to MY router.

Billing had no records of the third tech not being able to achieve the speed on his phone, nor any info regarding his boss re-provisioning the line and making it better but not fixing it, three modem replacements, or any subsequent local and neighborhood testing and home visits by five more technicians, one of them twice.

He said that there was *nothing he could do* for me. That sounded like an echo to me as I may have heard that before from you. I am going to suggest those six words as a motto for your corporation.

I know that this technical issue has not yet resolved but it looks like some intervention in updating the recordkeeping is going to be required for me to eventually come to terms with your billing. Am I on the hook for the next seven service calls and you just have not billed me yet?

Got The Spectrum Billing Blues

Got your bill today and I did learn
You charged me for what you did not earn
Called your billing to complain
There's nothing we can do was their refrain
Chorus: It's not us, it's you
There's nothing we can do
Waited on hold for your support
Then support joined me on hold for their support
So apparently karma is still alive and well
We all get to live in Spectrum hold queue hell
Chorus: It's not us, it's you
There's nothing we can do
Billing can only go by the notes in the file
But it's your lack of notes that I revile
You got off easy in your lawsuit in New York
Yet the bill you send me is full of pork
Chorus: It's not us, it's you
There's nothing we can do

Well, since this saga has been going on for so long now, it is about time for a summary on where we stand, nowhere, and for me to provide some additional information.

Update

Got a call today from Spectrum Regional Field Service Mgr., Eastern Wisconsin, 39 days into this and still counting. Had a chat, but he remains unconvinced that the problem is the network and not me. So I sent him some additional info and we agreed to chat later in the week, which by the way did not happen. No response to my emails either, just more one-way correspondence with Spectrum.

In addition to providing you with new information on my contact with billing, I have included my previous *one-way* email correspondence with one of your Field Supervisors for you to review.

Below is a brief, for me, summary of my experiences with Spectrum technical support over the past six weeks to this point in time.

The Cast of Characters responding to my speed complaint in order of appearance at my home:

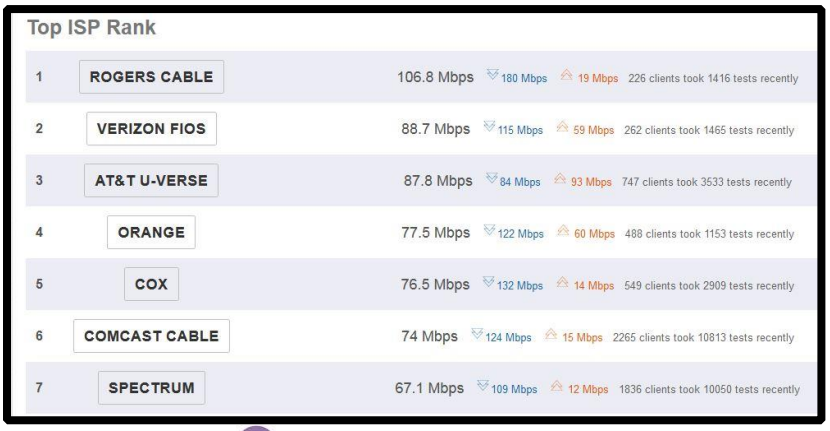
1. **J. did not have a laptop with which to test. Used his phone to get the provisioned speed. Said there was nothing else he could do.**
2. **P. had a laptop but did not use it. He said he had tried this before and could not get provisioned speed at modems with his laptop but did not know why. He actually refused my invitation for him to do so. He ended up using his phone to get the provisioned speed from my router that he pronounced bad (stuck). I showed him that my computer could not, but he said there was nothing else he could do.**
3. **C. did not have a laptop to use to test. Used my laptop years ago to install my service and this annoyed me then, and still does now. Used my computer and his phone here and could not get provisioned speed. He called his boss and got this whole new process moving.**
4. **W. could not achieve provisioned speed on wireless, wired to router or modem with his HP laptop. Said there was nothing else he could do.**
5. **J. R. could not achieve provisioned speed on wireless, wired to router or modem with his HP laptop. Also not at neighborhood PED's.**
6. **B. did not bring a laptop to the party, just questioned, and blamed my equipment.**
7. **J. S. could in fact consistently get provisioned speed on his Dell laptop wired/wireless and phone wired/wireless, but only for a 30 sec. duration at only one test site.**

The true worth of an ISP

https://testmy.net/legit-speed-test.php

In our opinion, the true value of an Internet service provider, ISP, is not always measured in megabits. Truly great providers maintain good peering relationships with other providers so their users sustain quality speeds throughout the Internet, not just nearby.

What good is an Internet connection if you can only get your advertised speeds on your provider's internal network (or on the edge of their network). It is the **Internet not INTRAnet, t**hat you are paying them monthly for. If you run a speed test elsewhere and get higher results than you get here, poor provider peering may be to blame.

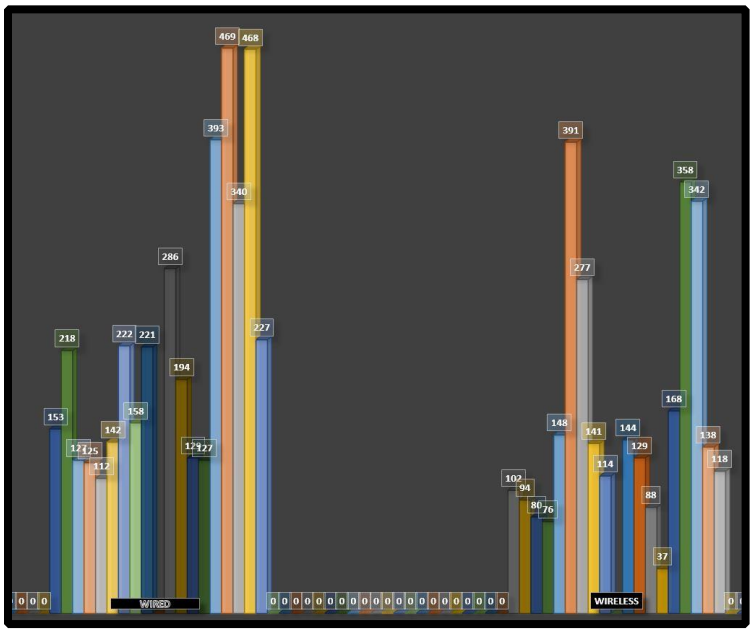


https://testmy.net/hoststats

Dear, Dear, Dear, and yet again Dear Spectrum

(The final side/episode of a double album set, I hope, and yet you made me write another 6000 words)

Continuing with the theme from my last email, "It's you and not me," what is seen below is a visual representation of my speed test data provided to you previously in an Excel worksheet.



The numbers in the chart above represent the Mbps speed achieved.

As you can see, only in two of the tests was the provisioned speed achieved when wired to the router via Cat7 cables. Both of these were on the Random Lake (Spectrum Intranet) test site. The highest speed achieved on the Wisconsin Rapids site was 222Mbps well short of the provisioned speed.

No tests on the wireless category achieved the provisioned speed, nor were they expected to, despite the computers being placed within four feet of the router. The highest readings were again achieved on the Random Lake speed test site, or in other words the Charter/Spectrum Intranet.

In addition, twenty-two speed test sites shown in the graphic below, all default to Renaissance Learning, Inc. Wisconsin Rapids, WI as the optimal speed test site. Using my Spectrum Internet connection, this test site shows lower speeds than the preferred site of Spectrum technicians, Random Lake Charter/Spectrum Intranet.

https://myspeedcheck.net/speedtest/Mediacom (click on the chart to follow.)

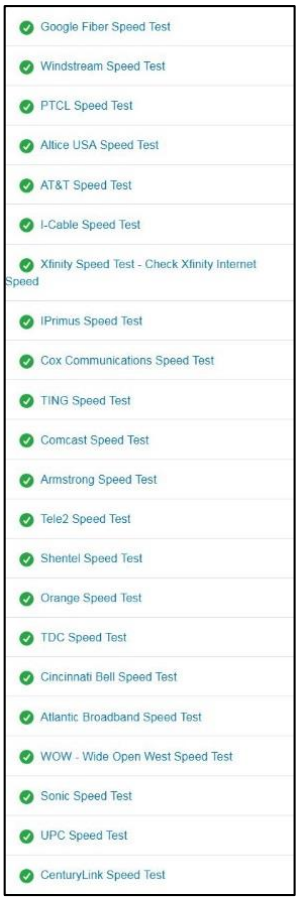
The Real Digital Divide? Advertised Vs. Actual Internet Speeds

Our data shows that 15% of Internet users in the U.S. — nearly 45 million people — are not getting the speeds they're paying for. On average, Americans are getting 79% of the speed they pay for.

Cable and fiber are by far the most common home Internet connections in the U.S., but they are also the most likely to under-deliver, with most people getting only a quarter of the speeds they are paying for.

Allconnect's internal data shows that cable and fiber Internet providers advertise faster speeds than they actually deliver, while the FCC's report shows the opposite.

https://www.allconnect.com/blog/advertised-vs-actual-Internet-speeds



Research from Purdue University FCC/M-Lab Speed Ratios

Table shows average advertised FCC speeds* as well as average test speeds from M-Lab. The download and upload ratios were calculated by dividing the FCC speed by the M-Lab speed.

https://pcrd.purdue.edu/the-real-digital-divide-advertised-vs-actual-Internet-speeds/

Meanwhile where I live:

Avg. M-Lab Download (Mbps)	Avg. M-Lab Upload (Mbps)	FCC Avg. Download (Mbps)	FCC Avg. Upload (Mbps)	Download Ratio	Upload Ratio
25.859	5.798	146.063	10.775	5.6	1.9

**According to the Federal Communications Commission (FCC) Form 477 ISP self-reported dataset—which is historically been proven to significantly overestimate both availability and the speeds provided by Internet providers.*

When I mentioned my issues with getting Netflix and Amazon Prime Video to play in HD, and wondered which of them was throttling me, the Spectrum Field Sup. Mgr. told me that they do not throttle speed. But then one needs to ask why does the below exist in your residential Internet acceptable use policy?

Charter uses a variety of reasonable network management tools and practices consistent with industry standards. In the event the periods of congestion necessitate such management, Charter has available the following tools and practices (without limitation and as may be adjusted over time): (i) use of an upper limit of bandwidth allocated for uploading of files during congested periods; (ii) Subscriber Traffic Management (STM) technology to temporarily lower the priority of traffic with the greatest impact on peak congestion; (iii) spam filtering and detection techniques; and (iv) measures to protect the security and integrity of its network, resources and subscribers. In limited instances if employed, **these techniques may affect the throughput rate at which subscribers may send and receive data**, the ability of users to establish session connections within the network, or result in the delay of certain traffic during times of peak congestion.

https://www.bandwidthplace.com/bandwidth-throttling-and-your-spectrum-Internet-service/

Here is an interesting take on your business model that I ran across online.

"They oversell their capacity on the basis that there won't be a time when everybody uses it at once. The phone companies have been doing this for years. There are network planners who work out exactly how much capacity they need to stay ahead of demand.

There is a limit based on hardware within the ISP. This is much larger than any one user, but it is likely to be much less than the sum of all the provisioning for all the users. This works much like bank deposits do - the ISP depends on the users not demanding their full bandwidth all at the same time.

How much total speed to they have? That is hard to answer because it is not a single really big connection. They might have terabits of connection to some ISP's and only 10 or 100 gigabits to others.

ISPs get the bandwidth they sell from IXPs, or Internet Exchange Points, and transport it to customers. At each IXP, they are able to meet and exchange traffic with a set of other ISPs.

So the total amount of bandwidth an ISP has to sell is the sum of the bandwidth it's able to deliver to and from all IXPs combined, less any inefficiencies due to lack of interconnections (peering) at those IXPs, plus a little bit because occasionally the ISP's own customers will want to talk to each other, and that traffic doesn't need to go to an IXP and back. Speed x distance = cost.

The closer a customer is to the IXP they are using bandwidth from, generally speaking, the faster their connection will be at a given price. But since customers generally want to use bandwidth from a lot of different IXPs, and do not distinguish between them, in reality each customer is getting a blend of bandwidth sourced from IXPs all over the world.

A good ISP is going to have multiple connections with the greater Internet -some combination of direct ISP-to-ISP connections, or ISP-to-datacenter, or ISP-to-Internet-exchange.

This means that they'll try a variety of mechanisms to prevent excessive use by a few customers from making too many of the well behaved customers from leaving for another ISP, calling the help desk, filing trouble reports, or even (in the rare case where it's possible) jump to another ISP.

They want enough capacity to keep the revenue stream flowing and deal with some peaks, but not waste money providing peak service that's rarely used. It is like a fast-food restaurant pre-making fries or burgers

to anticipate a lunch rush - keep the customers happy but do not have too much waste at the end of the rush.

The further you get away from the customer, the less meaningful the idea of a "total divided to users" is. It works best on a neighborhood basis. It might work OK on a city basis, if the ISP has only a single main connection to its infrastructure. It barely matters across something the size of a US state. Not at all across a country. And is laughable across a continent."

https://www.quora.com/How-ISPs-determine-speed-for-the-users-What-is-the-total-Internet-speed-an-ISP-has-and-according-to-what-it-gets-divided-to-users?share=1

"While the infrastructure and services provided by Spectrum have seen high ratings, their reputation with the Better Business Bureau (BBB) is less promising. The BBB gave Spectrum an **F** rating, the lowest grade possible. This measurement seeks to evaluate how a company interacts with its customers and can reflect a company's customer service. The biggest drawback to Spectrum Internet is its history of poor customer service, as evidenced by its BBB and J.D. Power reports. Spectrum's monthly fees are also a bit higher than other cable providers."

https://www.reviews.com/utilities/Internet/charter-communications-review/

43 US Internet Exchange Points

Phoenix-IX - The Phoenix Internet Exchange	Phoenix, AZ	USA	N/A	
TIE-PHX - Telx Internet Exchange Phoenix	Phoenix, AZ	USA	1	
CIIX - CENIC International Internet eXchange	Los Angeles, CA	USA	1	
EQIX-LA - Equinix Exchange Los Angeles	Los Angeles, CA	USA	2	
LAIIX - Los Angeles International Internet eXchange	Los Angeles, CA	USA	1	
PAIX-PAO - Peering And Internet eXchange Palo Alto	Palo Alto, CA	USA	4	
SFMIX - San Francisco Internet eXchange	San Francisco, CA	USA	1	
EQIX-SJC - Equinix Exchange San Jose	San Jose, CA	USA	2	
IX-Denver - Interconnection eXchange - Denver	Denver, CO	USA	N/A	
TMRK-MIA - Terremark NAP of the Americas	Miami, FL	USA	1	

TampaIX - Tampa Internet eXchange	Tampa, FL	USA	N/A	
TPA-IX - Tampa Internet Exchange	Tampa, FL	USA	2	
PAIX-ATL - Peering And Internet eXchange Atlanta	Atlanta, GA	USA	1	
TIE-ATL - Telx Internet Exchange Atlanta	Atlanta, GA	USA	1	
ChIX - Chicago Internet eXchange	Chicago, IL	USA	1	
EQIX-CHI - Equinix Exchange Chicago	Chicago, IL	USA	2	
Midwest-IX - Midwest Internet Exchange	Indianapolis, IN	USA	3	
KCIX - The Kansas City Internet Exchange	Kansas City KS, KS	USA	2	
BOSIX - Boston Internet Exchange	Boston, MA	USA	1	
DET-IX - Detroit Internet Exchange	Detroit, MI	USA	3	
MICE - Midwest Internet Cooperative Exchange	Minneapolis, Minnesota	USA	1	
OmahaIX - Omaha Internet eXchange	Omaha, NE	USA	1	
LINX-NoVA - LINX North Virginia	Washington D.C., North Virginia	USA	3	
Big-APE - The Big Apple Peering Exchange	New York, NY	USA	1	
EQIX-NYC - Equinix Exchange New York	New York, NY	USA	3	
NYIIX - New York International Internet eXchange	New York, NY	USA	3	
PAIX-NYC - Peering And Internet eXchange New York	New York, NY	USA	3	
TIE-NYC - Telx Internet Exchange New York	New York, NY	USA	2	
iX-OKC - Internet eXchange Oklahoma City	Oklahoma City, OK	USA	N/A	
OIX - Oregon Internet Exchange	Eugene, OR	USA	N/A	
SOAX - Southern Oregon Access Exchange	Medford, OR	USA	1	
NWAX - The Northwest Access Exchange	Portland, OR	USA	2	
PitX - The Pittsburgh Internet Exchange	Pittsburgh, PA	USA	N/A	
DECIX-Dallas - DE-CIX Dallas Fabric	Dallas, TX	USA	N/A	
EQIX-DAL - Equinix Exchange Dallas	Dallas, TX	USA	1	

PAIX-DAL - Peering And Internet eXchange Dallas	Dallas, TX	USA	2
TIE-DAL - Telx Internet Exchange Dallas	Dallas, TX	USA	2
MEX-IX - MEX-IX McAllen	McAllen, TX	USA	N/A
EQIX-ASH - Equinix Exchange Ashburn	Ashburn, VA	USA	4
PAIX-VIR - Peering And Internet eXchange Virginia	Vienna, VA	USA	1
PAIX-SEA - Peering And Internet eXchange Seattle	Seattle, WA	USA	2
SIX - Seattle Internet Exchange	Seattle, WA	USA	1
MadIX - Madison Internet eXchange Peering Point	Madison, WI	USA	N/A
MKE-IX - Milwaukee Internet Exchange	Milwaukee, WI	USA	N/A

****UPDATE****

I had a call today from a Spectrum VP regarding my issues. She seemed genuinely interested and yet uninformed regarding my latest communications and test data, or pretended to be in an attempt to hear my side of the story directly from me. She told me that she had removed the truck roll charge from my bill, and that these charges are automatically applied unless the technician removes them. Automatic opt in, no notice, how nice.

She asked me what I wanted and I told her 1Gbps symmetrical fiber to my house and to grow up to be George Jetson. But seriously, I explained how the price is too high for the limited service, and that I am looking for a discounted rate, as I am now sure that Spectrum cannot actually deliver 400Mbps to my house. Also that I am highly confident that based on my testing, and that this is not the fault of my equipment.

If the Spectrum 400Mbps service is only available to specific types of computers, phones, or Internet browsers, and then only to one Random Lake test site (Spectrum Intranet), then their advertising should reflect those conditions and stipulations.

She was primarily looking to find a resolution to this issue. She agreed to further consult with her team, look further into the issue, and get back to me later this week. Meanwhile I will provide some additional info.

Spectrum Internet Plans and Prices

Plan	Download Speeds up to	Price per month
Spectrum Internet	200 Mbps	$49.99
Spectrum Internet Ultra	**400 Mbps**	**$64.99**
Spectrum Internet Gig	940 Mbps	$104.99

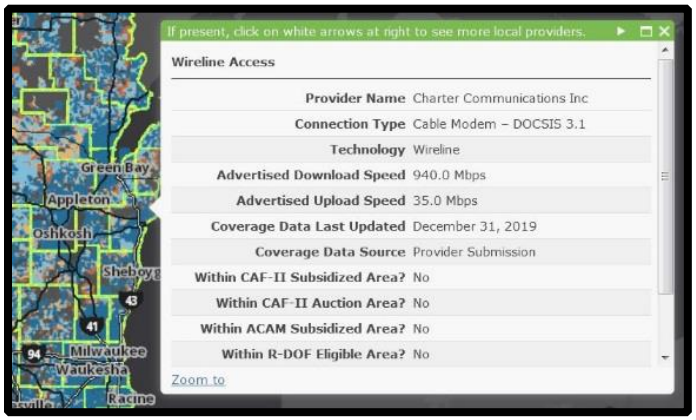
Data effective 1/19/2021

Remember the competitive examples from the previous email?

Here is what your competition would be like if we had a free and open market. You know what I mean, that whole invisible hand of the free market thing businesses like yours like to talk endlessly about.

- Verizon FiOS Gigabit 940/880 Mbps speeds $69.99 /mo.
- AT&T Internet 1000 940/880Mbps $60 /mo.
- Gigabit Internet by XFINITY from Comcast 1 Gbps/35 Mbps $70.00 /mo.
- Gigabit Pro by XFINITY 2Gbps/2Gbps (Fiber To The Home (FTTH) **OMG!**

According to the Wisconsin Broadband map, Spectrum offers 940Mbps in my state but cannot even provide 400Mbps to me?

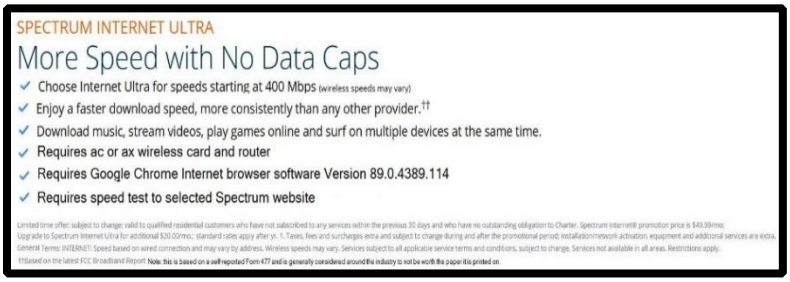


https://maps.psc.wi.gov/apps/WisconsinBroadbandMap/

Given the current Spectrum plan above, I do not understand why I should be paying **$94.99** for what appears to be a fairly reliable 200Mbps connection, but not the promised 400Mbps.

It seems like your installation system is setup to provide a false and phony reading on a phone via a Spectrum **Intranet**. This is exactly what the first and second on-site technicians did here at my home.

A more realistic speed testing process would involve a Charter FTP server located at your first hop datacenter. This site could then be used to download sample 1GB files for testing actual download speed, at least to your first hop. Again, this whole idea of testing to a *local* server is an outdated and inaccurate historical remnant of the cable TV days of providing local cable television service to the home.



I believe that your advertisements should look more like this:

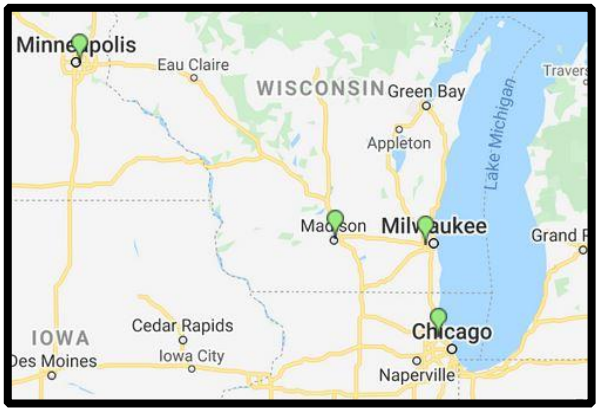
https://www.spectrum.com/ultra (proposed)

Failing that approach, a speedtest.net site should be located on one of your network servers at your first hop of 096-034-023-212.biz.spectrum.com 96.34.23.212. IP2Location puts this at Fitchburg, WI. This appears to be an IXP and would be a much more realistic test in my mind.

When you stop and think about it, I am paying Spectrum for a connection to the Internet, not a Charter/Spectrum Intranet connection. My email and webservers are in Milwaukee. I am paying for a connection to the Internet backbone IXP, not to some random server in Random Lake.

About Internet Exchanges

An Internet exchange or IXP is a switching platform where Internet carriers can exchange peering traffic with each other. Exchanging peering traffic over an Internet exchange point rather than via direct peering enables a carrier to interconnect with multiple networks via one uplink and thereby reduce the cost and complication of peering.



In having my volunteered assistance in troubleshooting this problem over the past few months, I have asked all three of the Field Supervisor Mgrs. who came to my home the same two questions:

Is there anyone else in my node who has Internet provisioning above the standard 100mbps service?

How far away from my location, does the fiber out of your office terminate and get changed over to copper?

Both of these questions seem to me to be important in troubleshooting the problem. Yet the answer to both questions from all three was, "I don't know." I might be able to understand if they do not want to say for some valid reason, proprietary corporate info, privacy, Homeland Security issues, their personal risk of possible offsite rendition if they tell, etc., but the answers should be that then. They did say that there are 210 devices on the local node. I have 10 of those myself.

The Field Supervisor Regional Manager when asked also did not know these answers but said that this information was in fact available to the Field Supervisor Mgrs. on their hand held devices. Go figure.

****UPDATE****

Got a voice mail today from the Field Supervisor Regional Manager (FSRM) saying that they were still analyzing the data and info that I sent them (or plotting my demise?) and would get back to me on Monday. Sent him an email agreeing with this plan and a note that since I am waiting until Monday to speak to him and not the VP, I am sending more info and I am a bit disappointed. No offense to you but I thought your boss and I hit it off over the phone yesterday, as we agreed on some things, and I made her laugh on a number of occasions. Yet another Charter unrequited love story I guess. Since we have only just met it is too soon to write a blues song about this one however.:-)

Since I had some more time, I did some more digging. More testing today. 14 hops to anywhere.

I have discontinued the use of the Open Visual Trace Route software since the Geo location has been inaccurate. Open Source Software-everyone can look at it, but no one apparently does.

I was working on my website today and had occasion to download a large file. I tracked the results and display them below. So in summary I am seeing a 50Mbps download, albeit via a wireless connection which reports in the 80Mbps range on the speedtest.net sites.

50.4Mbps FTP speed with a 775 MB file down from Cyberlynk.net using WS_FTP software.

In thinking more about my slow FTP (file transfer protocol) like IP (Internet protocol) only different, I decided to run a trace route on Cyberlynk.net , below where my website is, and compare it to the trace route I sent you earlier to Spectrum.com below. The good news is there is four less hops, but my packets have to bounce around Wisconsin, and then visit California and Texas before getting to cyberlynk.net in Franklin after one last stop in Chicago. I would like Spectrum to get me 400Mbps to an IXP like Madison or Chicago without chasing around the state and around the country. Remember that a trace route only gives you a small part of the overall picture and does not show delays really. I wish I had visibility into your peering agreements. I think I could fix this for you. ☺

Tracing route to cyberlynk.net 66.185.30.186

96.34.23.212 Fitchburg Wisconsin
96.34.30.25 Wausau Wisconsin
96.34.24.83 Eau Claire Wisconsin
96.34.24.136 Eau Claire Wisconsin
96.34.2.153 Riverside California
96.34.3.55 Dallas Texas
4.68.38.253 Dallas Texas
4.14.170.82 Chicago Illinois
66.185.29.234 Franklin Wisconsin

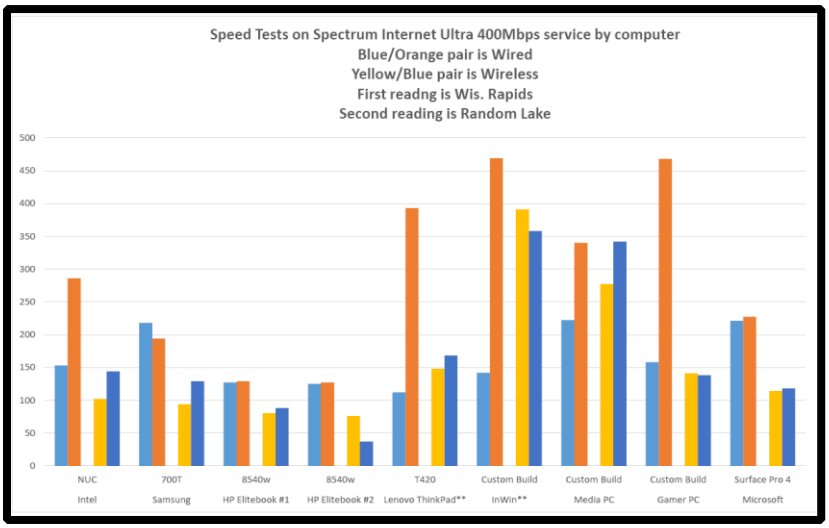
Trace route to spectrum.com 142.136.168.58

96.34.23.212 Fitchburg Wisconsin
96.34.30.25 Wausau Wisconsin
96.34.24.83 Eau Claire Wisconsin
96.34.24.136 Eau Claire Wisconsin
96.34.2.153 Riverside California
96.34.0.7 Ashburn Virginia
96.34.0.9 Ashburn Virginia
66.109.1.18 Chicago Illinois
66.109.6.21 Chicago Heights Illinois
66.109.10.99 San Jose California
66.109.10.93 San Jose California
66.109.6.245 Atlanta Georgia
165.237.51.245 Greenwood Village Colorado
165.237.4.131 San Jose California

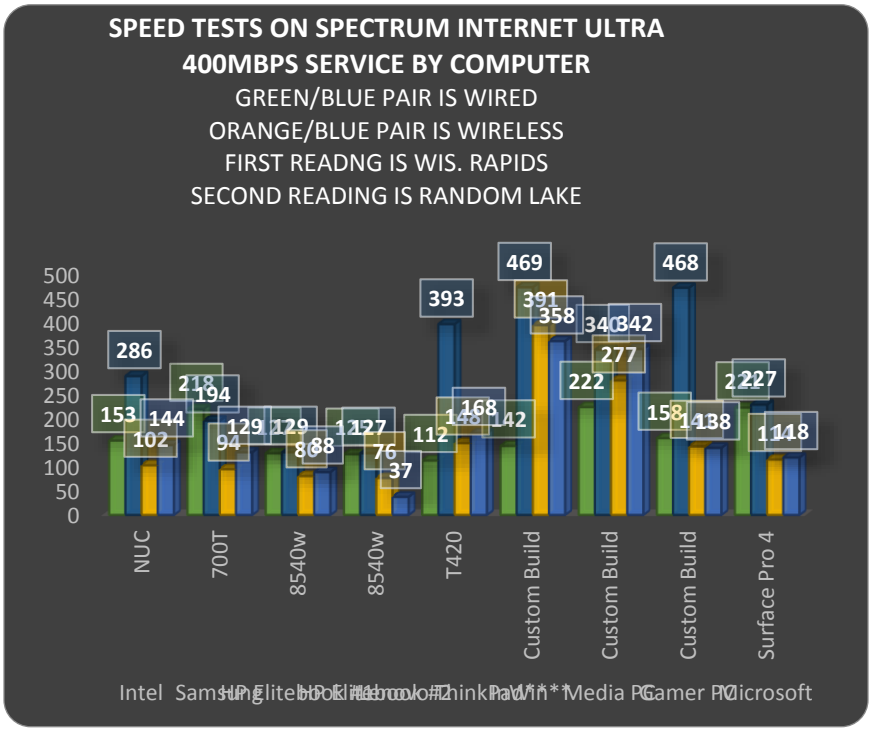
Note: Geo locations from https://www.iplocation.net/ip-lookup

66.185.30.186 Franklin Wisconsin

I also came up with what I think is a better visualization of my slow speed situation.



And another even better one:



At this point, I am feeling a bit like the loveable doofus Clark Griswold who took his family on an arduous, humorous, and disaster filled cross-country sightseeing automobile trip from Chicago to Los Angeles. They suffered tremendously on this journey on a persistent quest to enjoy a planned day at the theme park Wally World, only to find it closed for maintenance.

Or perhaps I am more like Don Quixote, a self-appointed knight thinking he can right the wrongs of corporate Internet monopolies, but is actually just riding full tilt against corporate windmills.

But maybe, just maybe, I should be feeling like Ed Snowden discovering deep and dark dirty hidden secrets, like modified Spectrum test equipment reflecting inaccurate overly positive speed test results. Are some or all of Spectrum technician issued phones as well as some Spectrum technician issued laptops modified? Are these Java software applets or scripts and/or possibly the Chrome browser software modified at the server, client, or both? Why did the FSSMgr test my speed successfully, plugged into my router rather than their touchstone, which has always been at the modem? Why was he so sure he could get the provisioned speed with his phone and laptop?

Why can't 11 of my devices 2 phones, 2 tablets, 3 laptops, 4 desktops consistently achieve provisioned speeds even at test sites within 100 miles of me? Why couldn't 4 of their devices (3 laptops/1phone) achieve it? Yet there are 5 of their devices that could in fact consistently obtain provisioned speed (4 phones/1 laptop? Inquiring minds want to know.

No call as promised today, just crickets. Are they still plotting my demise?

Got a call from Spectrum Customer Retention today. They offered me a discounted rate off their standard service rate (not the higher Ultra rate) for 12 months and then a discounted rate going forward to infinity. They also wiped my account balance to zero. This is a positive note on the billing end. Now what is going to happen on the technical provisioning end remains to be seen.

Got an email from the FSSRMgr questioning the source of the test data that I sent him previously. He made no mention of the missed phone call, (these people just do not talk to each other) and the test data source was clearly identified in what I sent him, but I sent it to him again. Stalling or busy?

Got a call from the FSSRMgr late in the day and he indicated that he had intervened with Customer Retention and was following up to see if they had contacted me. I said thanks and that they had made me a fair offer, which I accepted. He also said that he has been very busy but has been reviewing the materials I have sent. The VP is traveling but will try to call me in the next couple of days.

Got a call from the VP; the theme of the call was what the "End User Agreement" says. No promised speed to the Internet, just a vague promise of a connection to any location up to 70% of 400Mbps. I questioned the integrity of their test site; she proclaimed the virtue of the entire corporation, despite the lawsuits, "F" ratings in customer service, and the FCC basically saying that they did not trust their self-reported coverage and speeds. In the end, I said that we would have to agree to disagree.

But I guess for now that whole Cable TV service mentality will continue to prevail at Charter/Spectrum. It appears as if some FCC/FTC/State Attorney's General intervention will be required here to mend this potential monopoly behavior and alleged fraud.

So this will be my final letter Dear Spectrum. I will allow the FCC, FTC, and the Wisconsin DATCP and perhaps the Wisconsin Attorney General to take this issue from here.

Executive Summary

(Seems appropriate after me spilling some 20,000 words across four letters and two months on this saga)

- Late February I upgraded to Ultra speed and did not get a noticeable speed bump from the original 100Mbps provisioning.
- Called Tech Support and they rolled a truck, replaced the modem, and said it was fine but my router was stuck. Still did not get it. Hitron modem.
- Called Tech Support again and they rolled a truck and said it was fine but my router was stuck. Still did not get it.
- Replaced my 5yr old $300 router with a new $350 one.
- Still did not get it so I called Tech Support again, and they rolled a truck and found out it was not fine, worked on some cable issues, had a supervisor re-provision over the phone and it improved but not enough.
- They rolled a truck FSS did some testing, was verbally abusive, changed the modem, but found out it was not fine. Ubee modem.
- They rolled two trucks a tech and a different FSS did some testing, was a nice guy, changed the modem, but found out it was not fine. Testing with a laptop not good at my PED or in neighborhood either. Technicolor modem.
- They rolled two more trucks, a different FFS and FFSM sup Mgr., did some testing, were nice guys, but found out it was not fine except with their one laptop and phone on one test site. They pronounced it to be OK based on that. I still did not get it. I did have progress in a speed increase from about 150Mbps to 200-250Mbps during this time however.
- I wrote and emailed the first if four long letters to five of Charter Corp officers. Included lyrics for my first original song “Got the Spectrum Blues” with lyrics rhyming Spectrum to Rectum. The song blamed Charter/Spectrum and “hops” as the problem but also blamed LiMu Emu, Doug, Kevin Bacon and others. I also included a complete .mp3 audio recording file of these lyrics with BB King like guitar riffs and Chuck Berry like Honky Tonk piano licks.
- I produced a comprehensive testing spreadsheet of nine of my computers. Clearly showing I still did not get what I was paying for.
- Spoke multiple times on the phone, sent multiple emails to FSSRM
- Wrote the second letter providing more data and a semi-invented corporate meeting scenario as to why I suspected I could not get the advertised speed. More song lyrics.
- Wrote the third letter to provide more info, my contact with the FCC and FTC, and to whine about my encounter with your clueless Spectrum billing department. More song lyrics.

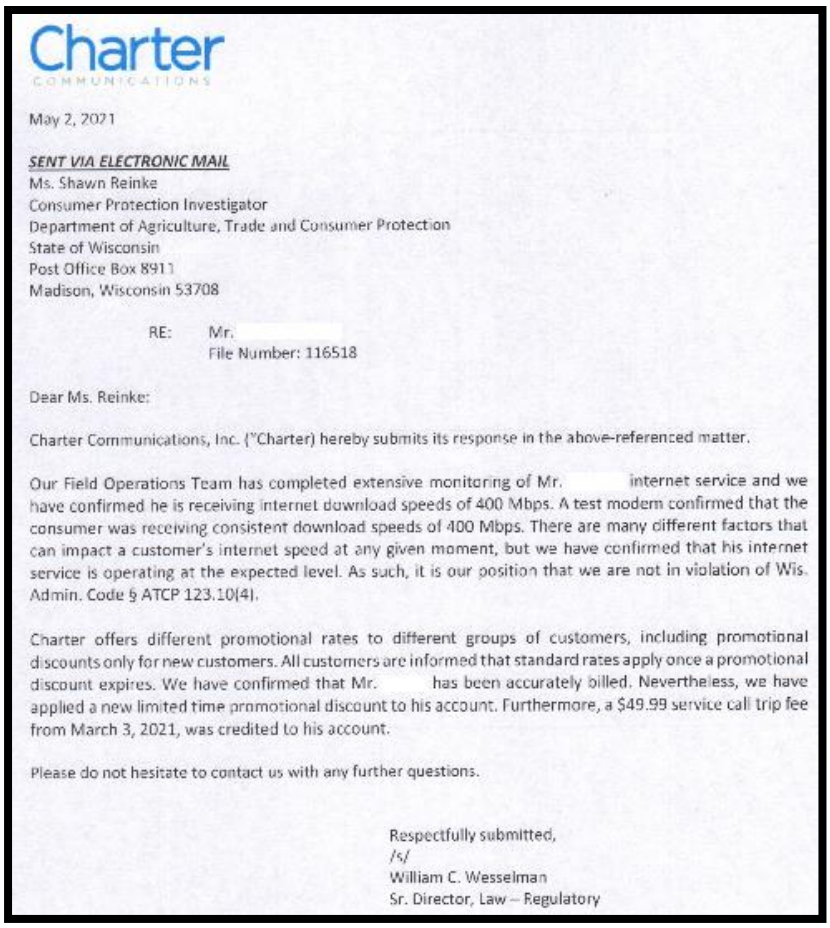
- Now you are reading the fourth and perhaps final letter providing some additional data, some speculation and accusations, and hopefully a conclusion to this saga.
- Spectrum Customer Retention made me a reasonable concession offer on monthly pricing. An admission of guilt, fault, or reality?

Over the course of four months and about 20,000 words, graphs, charts, test data, and song lyrics proving my case, I got them to improve my service from 100Mbps to 200Mbps on their Charter/Spectrum Intranet. I am still in the 50-100Mbps range getting to a Chicago backbone Internet connection.

They ended up discounting their 400Mbps rate to me for three years to the 100Mbps rate, which I see as an admission of guilt. This is the best they can do given their current cobbled together network architecture.

From contacting the Federal and State regulators, I got some lawyer letters from Charter.

The regulatory agencies are feckless in response and think that getting an unsubstantiated response from a corporation lawyer is doing their jobs. Not unlike the lying politicians on TV and one of the reasons that the world is as it is today.



Charter
COMMUNICATIONS

May 2, 2021

SENT VIA ELECTRONIC MAIL
Ms. Shawn Reinke
Consumer Protection Investigator
Department of Agriculture, Trade and Consumer Protection
State of Wisconsin
Post Office Box 8911
Madison, Wisconsin 53708

RE: Mr.
File Number: 116518

Dear Ms. Reinke:

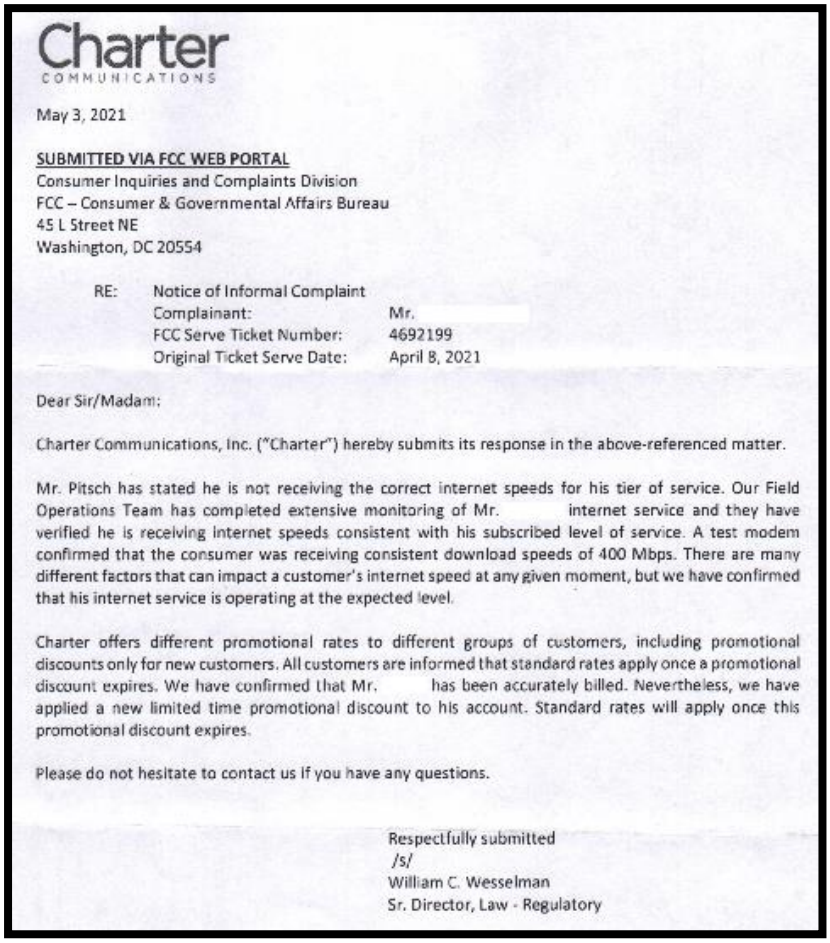
Charter Communications, Inc. ("Charter) hereby submits its response in the above-referenced matter.

Our Field Operations Team has completed extensive monitoring of Mr. internet service and we have confirmed he is receiving internet download speeds of 400 Mbps. A test modem confirmed that the consumer was receiving consistent download speeds of 400 Mbps. There are many different factors that can impact a customer's internet speed at any given moment, but we have confirmed that his internet service is operating at the expected level. As such, it is our position that we are not in violation of Wis. Admin. Code § ATCP 123.10(4).

Charter offers different promotional rates to different groups of customers, including promotional discounts only for new customers. All customers are informed that standard rates apply once a promotional discount expires. We have confirmed that Mr. has been accurately billed. Nevertheless, we have applied a new limited time promotional discount to his account. Furthermore, a $49.99 service call trip fee from March 3, 2021, was credited to his account.

Please do not hesitate to contact us with any further questions.

Respectfully submitted,
/s/
William C. Wesselman
Sr. Director, Law – Regulatory



Charter
COMMUNICATIONS

May 3, 2021

SUBMITTED VIA FCC WEB PORTAL
Consumer Inquiries and Complaints Division
FCC – Consumer & Governmental Affairs Bureau
45 L Street NE
Washington, DC 20554

RE: Notice of Informal Complaint
Complainant: Mr.
FCC Serve Ticket Number: 4692199
Original Ticket Serve Date: April 8, 2021

Dear Sir/Madam:

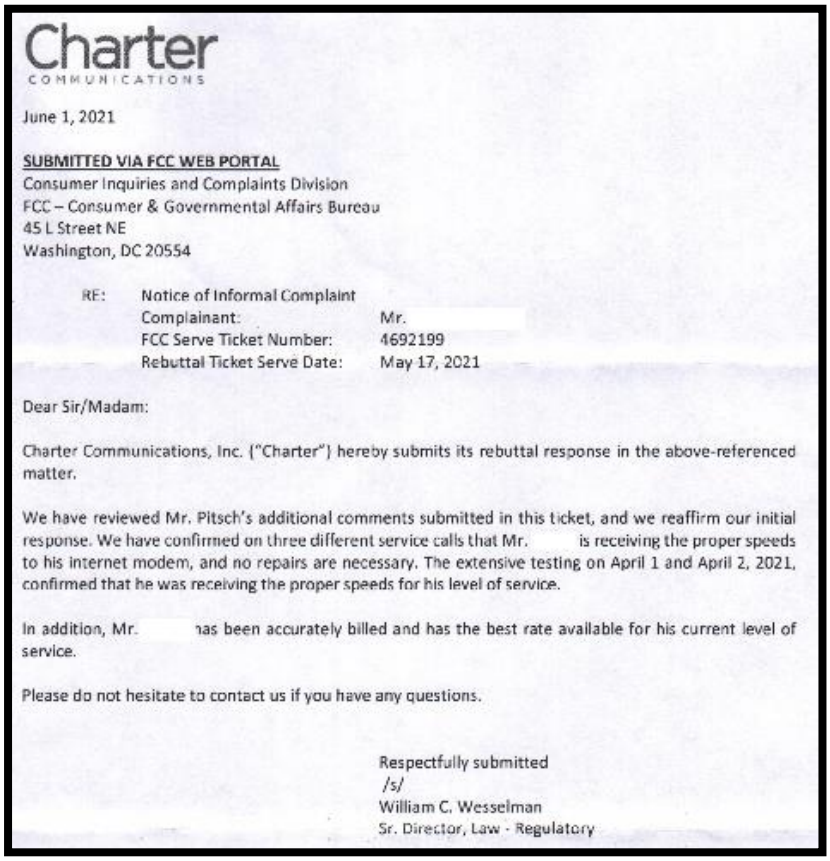
Charter Communications, Inc. ("Charter") hereby submits its response in the above-referenced matter.

Mr. Pitsch has stated he is not receiving the correct internet speeds for his tier of service. Our Field Operations Team has completed extensive monitoring of Mr. internet service and they have verified he is receiving internet speeds consistent with his subscribed level of service. A test modem confirmed that the consumer was receiving consistent download speeds of 400 Mbps. There are many different factors that can impact a customer's internet speed at any given moment, but we have confirmed that his internet service is operating at the expected level.

Charter offers different promotional rates to different groups of customers, including promotional discounts only for new customers. All customers are informed that standard rates apply once a promotional discount expires. We have confirmed that Mr. has been accurately billed. Nevertheless, we have applied a new limited time promotional discount to his account. Standard rates will apply once this promotional discount expires.

Please do not hesitate to contact us if you have any questions.

Respectfully submitted
/s/
William C. Wesselman
Sr. Director, Law - Regulatory



Charter
COMMUNICATIONS

June 1, 2021

SUBMITTED VIA FCC WEB PORTAL
Consumer Inquiries and Complaints Division
FCC – Consumer & Governmental Affairs Bureau
45 L Street NE
Washington, DC 20554

RE: Notice of Informal Complaint
Complainant: Mr.
FCC Serve Ticket Number: 4692199
Rebuttal Ticket Serve Date: May 17, 2021

Dear Sir/Madam:

Charter Communications, Inc. ("Charter") hereby submits its rebuttal response in the above-referenced matter.

We have reviewed Mr. Pitsch's additional comments submitted in this ticket, and we reaffirm our initial response. We have confirmed on three different service calls that Mr. is receiving the proper speeds to his internet modem, and no repairs are necessary. The extensive testing on April 1 and April 2, 2021, confirmed that he was receiving the proper speeds for his level of service.

In addition, Mr. has been accurately billed and has the best rate available for his current level of service.

Please do not hesitate to contact us if you have any questions.

Respectfully submitted
/s/
William C. Wesselman
Sr. Director, Law - Regulatory

Another word

(I never would have thought this would be necessary)

I have recently been sharing versions of this simple message with local, state, and federal leaders. I believe that this message applies to the future of your corporation as well. So I will leave you with these thoughts to ponder.

Politicians,

Now we must focus because we as a State do not want to miss out on the next wave of funding coming soon. $100 billion for broadband.

The restrictive laws you have put into place banning or restricting municipal and nonprofit Internet providers jeopardizes this funding I believe. It certainly contradicts the pending broadband funding priorities coming from the administration and eventually I believe from the FCC.

Coddling the incumbent monopoly providers who have promised and yet not delivered fiber optic cabling for the past thirty years have proven that the *invisible hand of the free market* does not work here, (if it actually works anywhere) despite 400 billion dollars plus of tax subsidies/grants/corporate welfare. http://teletruth.org/

My previous emails to you also reveal that these existing incumbent monopolies, i.e. Comcast, Charter/Spectrum, AT&T, do not now even consistently deliver the slower speeds, which they advertise and charge money for. I have filed complaints regarding this situation with the FCC, FTC, and WI DATCP. A closer inspection of these practices may well reveal fraudulent activities and/or monopoly behavior.

Meanwhile, we in rural Wisconsin need you to "get with the program" to promote the educational and employment opportunities, as well as the economic development that *real* rural broadband will bring. I do not mean the phony 25Mbps that the FCC calls broadband. I mean 1Gbps symmetrical fiber optic connections from the home or business directly to the Internet backbone.

If you think about this for a bit, this idea is not unlike the Great Lakes and Mississippi River ports, the railroad systems, the town, county, state, and Interstate highway systems, rural electrification, RFD postal service, and the public water and sewer systems of the past. These systems helped build this state. Economic development follows the infrastructure. Chickens lay eggs. It is a simple yet basic historical lesson.

PS. **Charter Must Pay $19 Million For Tricking Customers Into Switching ISPs (arstechnica.com)**

> *A judge has ordered Charter Communications to pay $19.2 million to Windstream for lying to customers in order to trick them into switching from Windstream to Charter's Spectrum Internet service. Charter also faces a $5,279 penalty for shutting off service to hundreds of Windstream's resale customers. Ars Technica reports: When Windstream filed for bankruptcy in early 2019, Charter began a "literally false and intentionally misleading advertising campaign intended to create the impression, using mailings designed to seem as if they were coming from the Debtors [Windstream], that the Debtors were going out of business," said an order issued Thursday by Judge Robert Drain of US Bankruptcy Court for the Southern District of New York. Charter's goal with the mailings "was to induce the Debtors' customers to terminate their contracts and switch to Charter by sending them literally false and intentionally misleading information about the Debtors' bankruptcy cases and financial wherewithal," the ruling said. Charter premised its ad campaign "on false assertions regarding the Debtors' bankruptcy cases," the ruling said.*
>
> *"We are gratified that Judge Drain's ruling means Charter will have to pay a significant price for its egregious false advertising," Windstream General Counsel Kristi Moody said, according to a FierceTelecom article. "Charter knew full well what it was doing when it embarked on a dishonest scare-tactic campaign to lure away our customers. At Windstream, we will always aggressively defend ourselves and our customers against predatory schemes and meritless allegations."*

Well, is that not just special!, says me.

PPS.

> *Federal Communications Commission member Michael O'Rielly argued that "Internet access is not a necessity or human right" and called this one of the most important "principles for regulators to consider as it relates to the Internet and our broadband economy."*

https://arstechnica.com/information-technology/2015/06/Internet-access-not-a-necessity-or-human-right-says-fcc-republican/?itm_source=parsely-api

I guess that depends are if you are looking at this from a 1% view or a 99% view. Are education, employment, housing, and inclusion in a participatory democracy human rights? Perhaps not, but maybe these rights are covered by that whole Life, Liberty, and the Pursuit of Happiness clause?

PPPS.

FCC Urges Americans To Run Internet Speed App To Counter Broadband Data Fudging (theregister.com)

> *The FCC is encouraging netizens to use its Internet speed mobile app in an effort to finally get accurate broadband data across the United States. The Register reports: In an announcement on Monday, the telecoms regulator noted that "the app provides a way for consumers to test the performance of their mobile and in-home broadband networks" and "provides the test results to the FCC." It stops far short of saying that the data will be used to make policy decisions, however, saying only that the figures gathered, "will help to inform the FCC's efforts to collect more accurate and granular broadband deployment data."*
>
> *The public push does not mean that things are going to get better soon. Big Cable has aggressively -- and successfully -- argued in the past that data provided by users over an app is not sufficiently robust to form the basis of governmental decisions. And so the FCC will have to use the results as a way to push for change rather than use the data to make direct decisions. Everybody, including numerous states, cities, congress folk and the GAO**, know that the official FCC data provided by ISPs is not worth the paper it is written on**. But broader usage of the app should expose just how inaccurate official figures are, which should in turn provide enough impetus for change. The bigger question is whether enough progress is made in the next four years to make any difference.*

PPPPS. (If there even is such a thing)

Striking Charter Workers Build ISP Where 'Profits Are Returned To Users' (arstechnica.com)

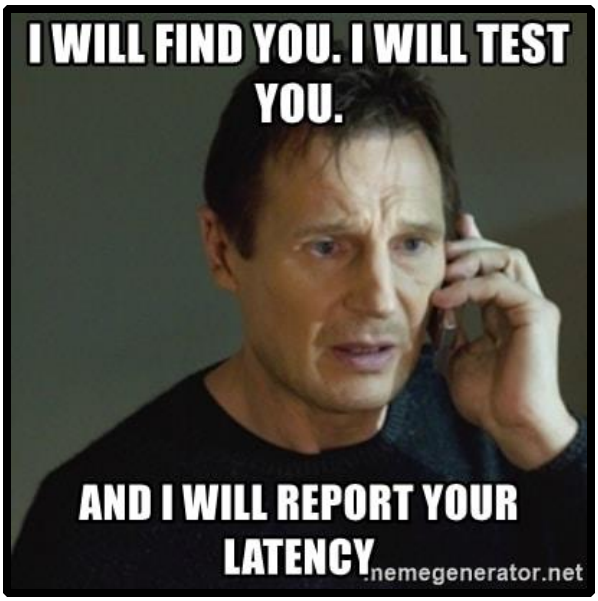
> *Charter Communications employees who have been on strike since 2017 are building an Internet service provider in New York City called "People's Choice." "People's Choice Communications is an employee-owned social enterprise launched by members of IBEW Local #3 to bridge the digital divide and help our neighbors get connected to the Internet during the COVID-19 pandemic," the ISP's website says. "We are the workers who built a large part of New York City's Internet infrastructure in the first place. We built out [Charter] Spectrum's cable system, until in 2017, the company pushed us out on strike by taking away our healthcare, retirement, and other benefits. It's now the longest strike in US history."*
>
> *So far, People's Choice says it has completed rooftop antenna installations at two schools in the Bronx and installed "hardline connections to wireless*

> *access points connecting 121 units" at housing for survivors of domestic violence who have disabilities. A Gizmodo article said the system is equipped to offer minimum speeds of 25Mbps downstream and 3Mbps upstream, meeting a broadband standard that has been used by the Federal Communications Commission since 2015. "We have a big portion of most of the Bronx covered with our antenna," IBEW Local #3 steward Troy Walcott told Gizmodo. "Now we have to go building by building to let people know we're out there and start turning them on." "A few dozen Spectrum strikers have been actively involved in the installations, but Walcott expects that at least one hundred workers are waiting in the wings for the project to scale up," the Gizmodo article said. "We work in affordable housing, supportive housing, co-op housing, NYCHA [NYC Housing Authority], homeless shelters, and regular old apartment complexes," the webpage notes. You can fill out this form if you are interested in bringing broadband to your building.*
>
> *"After we build out a network in your building, it transfers to cooperative ownership, so profits are returned to users," the People's Choice website says. "We are able to provide high-speed service in most cases for $10-$20/month. No more cable company ripping you off, and as an owner, you have a vote in policies like data privacy."*

It seems to me like Charter is in the news a lot lately and none if it seems to be too good.

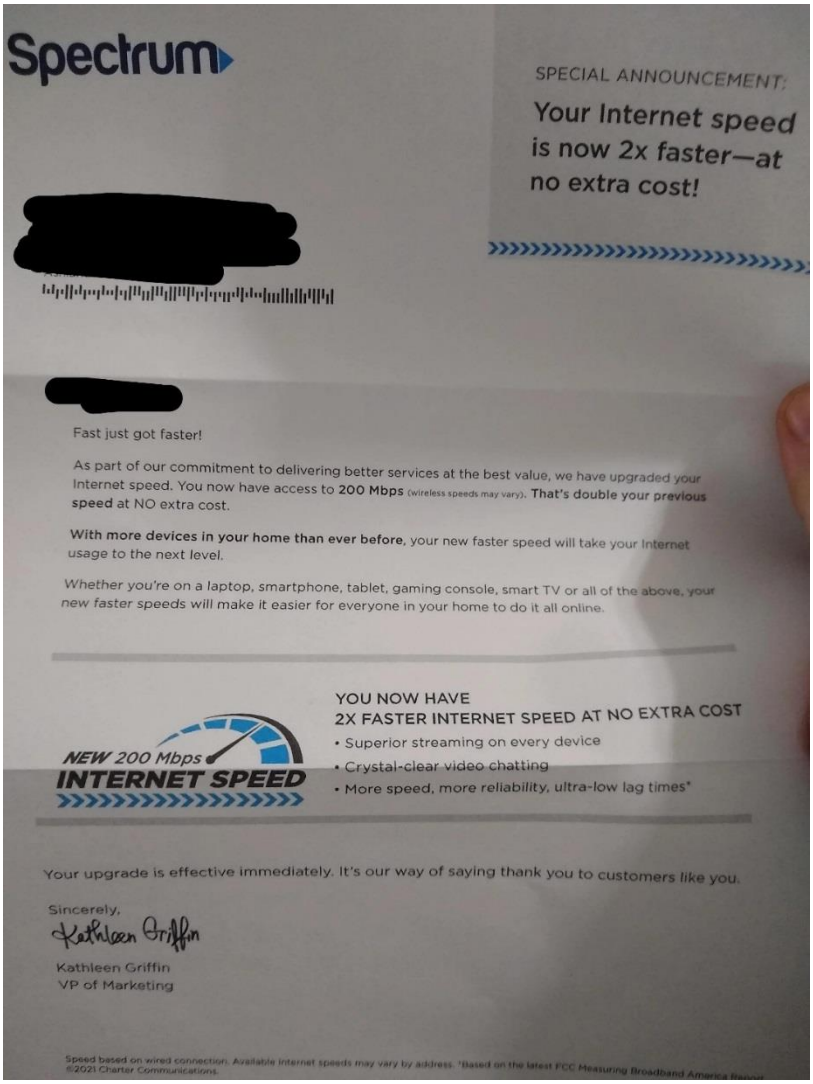
And finally…

"I know who you are, I know what you want. I can tell you that I do not have enough money for you... but what I do have are a very particular set of skills. Skills I have acquired over a very long career. Skills that make me a nightmare for corporations like you. I will find out about you, I will test your speed and latency, and I will report your shortcomings." (*A paraphrase of Liam Neeson as Bryan Mills in the movie Taken)*



BREAKING NEWS

I guess some lucky souls are getting this letter. This could have prevented my whole 2-month ordeal. Northeast Wisconsin is noticeably absent any of these letters.



Spectrum

SPECIAL ANNOUNCEMENT:

Your Internet speed is now 2x faster—at no extra cost!

[redacted]

[redacted]

Fast just got faster!

As part of our commitment to delivering better services at the best value, we have upgraded your Internet speed. You now have access to **200 Mbps** (wireless speeds may vary). **That's double your previous speed** at NO extra cost.

With more devices in your home than ever before, your new faster speed will take your Internet usage to the next level.

Whether you're on a laptop, smartphone, tablet, gaming console, smart TV or all of the above, your new faster speeds will make it easier for everyone in your home to do it all online.

NEW 200 Mbps INTERNET SPEED

YOU NOW HAVE
2X FASTER INTERNET SPEED AT NO EXTRA COST

- Superior streaming on every device
- Crystal-clear video chatting
- More speed, more reliability, ultra-low lag times*

Your upgrade is effective immediately. It's our way of saying thank you to customers like you.

Sincerely,

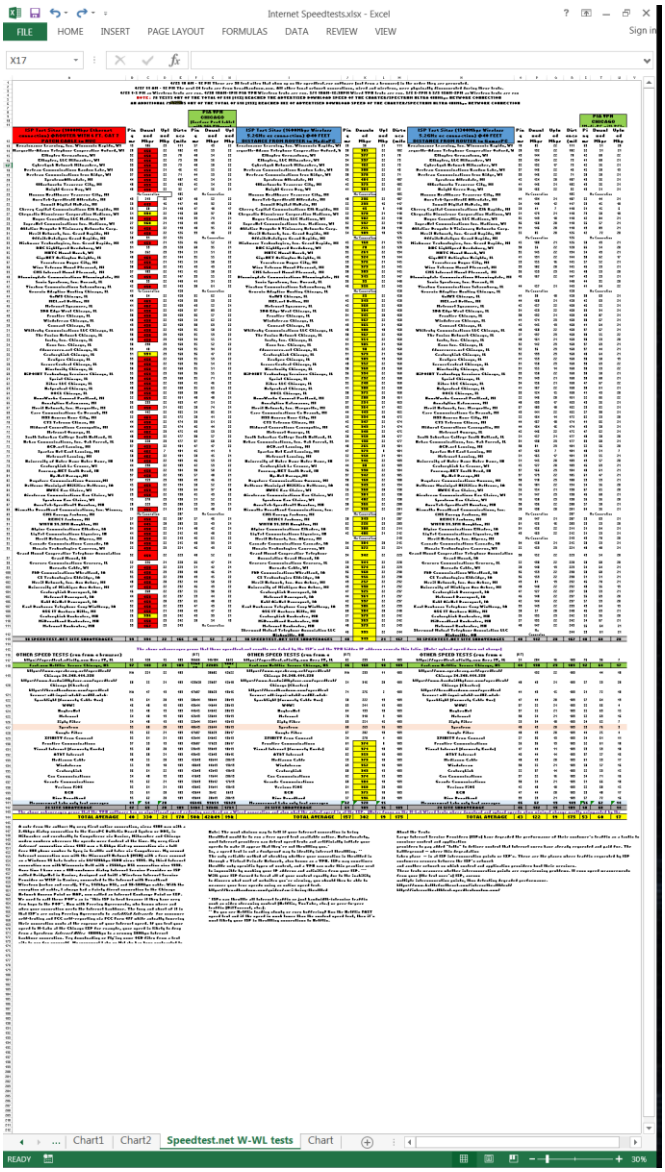
Kathleen Griffin

Kathleen Griffin
VP of Marketing

Speed based on wired connection. Available Internet speeds may vary by address. *Based on the latest FCC Measuring Broadband America Report
©2021 Charter Communications.

Ok Charter/Spectrum it is Time to Cut the Shit!

(The accompanying Excel spreadsheet shows that only 70 Tests Out Of 600 (12%) Reach the Advertised Speed of the Charter/Spectrum Internet Ultra 400mbps Network Connection)

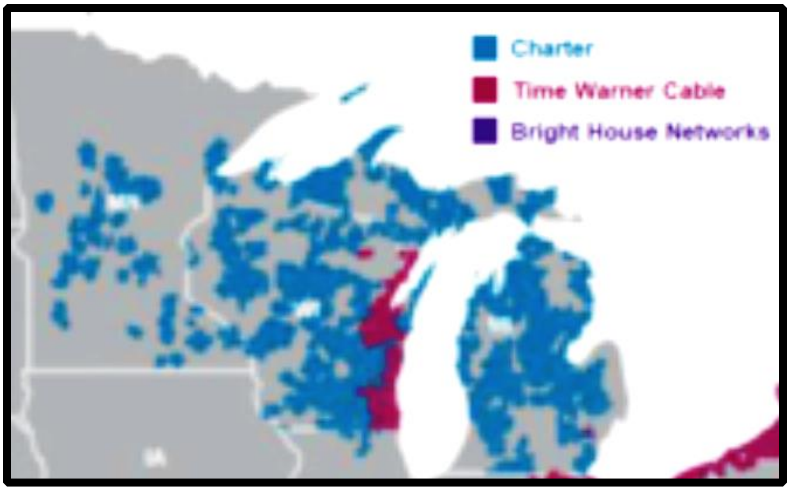


Let us begin here anew with a quote from a well informed Internet Service Provider or ISP, who has been in business for decades shall we? When surveyed and who, when shown a copy of my tracert to Spectrum.com said the following:

> *"Spectrum currently has two networks in Wisconsin. The old legacy Time Warner Cable, or TWC network and then they have a new Spectrum network for all of the NEW areas in Wisconsin they have built out.* ***From your geographical location, this new network takes your traffic the long way around the Spectrum Intranet network and through the Charter network to get you to the real Internet."***

As you can see, it can take 14 hops to get there.

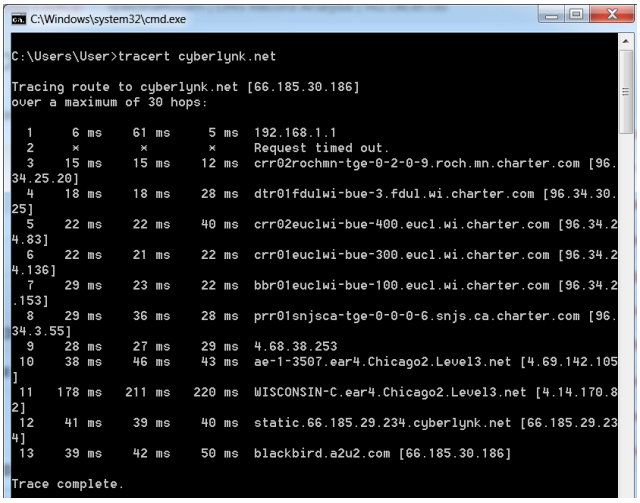
Trace route to spectrum.com 142.136.168.58
96.34.23.212 Fitchburg Wisconsin
96.34.30.25 Wausau Wisconsin
96.34.24.83 Eau Claire Wisconsin
96.34.24.136 Eau Claire Wisconsin
96.34.2.153 Riverside California
96.34.0.7 Ashburn Virginia
96.34.0.9 Ashburn Virginia
66.109.1.18 Chicago Illinois
66.109.6.21 Chicago Heights Illinois
66.109.10.99 San Jose California
66.109.10.93 San Jose California
66.109.6.245 Atlanta Georgia
165.237.51.245 Greenwood Village Colorado
165.237.4.131 San Jose California



Note: Geo locations from https://www.iplocation.net/ip-lookup

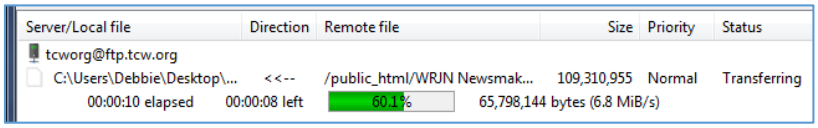
https://www.computerworld.com/article/2926226/charter-time-warner-deal-would-get-tough-regulatory-scrutiny.html

A tracert from my computers to my hosted website for example, goes something like from me to Fitchburg, Eau Claire, Wausau, LA, Dallas, Chicago, and then finally to Franklin. This appears to also prove out the above quote.



Or how about another quote from another ISP?

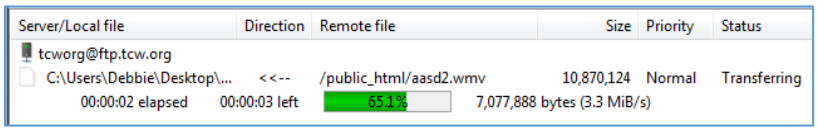
> *"We have no good way of knowing if traffic is being throttled somewhere or by who. All we have to go off of is from my desk the speeds are 600-900Mbps for FTP transfers and we are not hearing complaints from other customers."*



FileZilla 57Mbps

Or maybe one more quote:

> *"As for the FTP speeds, there is not much we can do on the uploads/downloads from your location. If there was a problem with the server or our datacenter network or with any of our five Internet connections, we would have thousands of customers complaining about speed issues."*



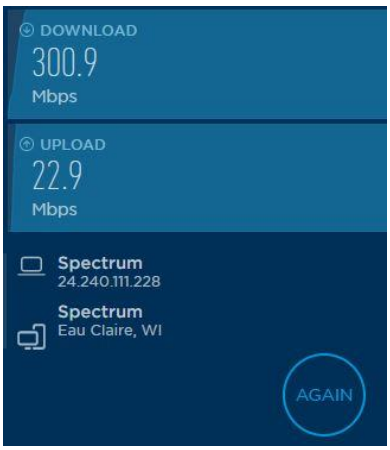
FileZilla 28Mbps

With regard to https connections:

On a wired 1000Mbps Ethernet connection, if you use a misleading speed test and do not venture too far (100 miles) from home:

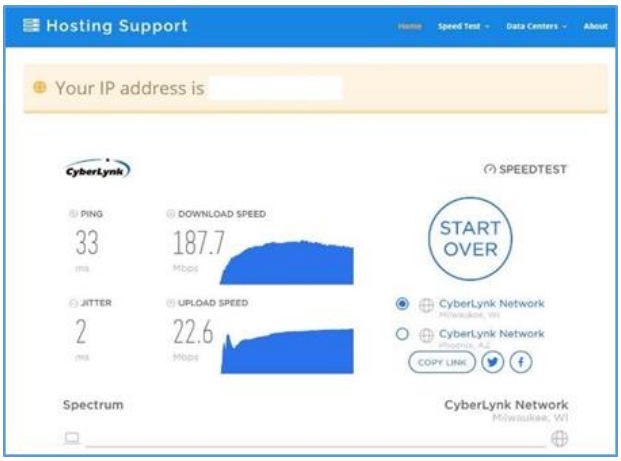
You will get something like this:

If your packets venture out towards the edge (200 miles) of the Spectrum Intranet:



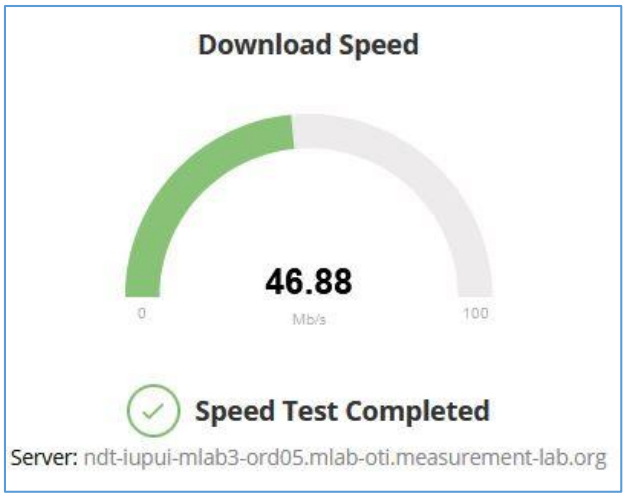
You start to lose your speed.

Then if you ping pong around the Charter/Spectrum Intranet to the actual Internet *going around the horn* as shown in the tracert, and then do a speed test at my Franklin website provider, hostingsupport.io, it shows:



This is gives you more of a “real world” Internet speed test.

Then when your packets were passing through Chicago, and they wanted to stop and test Charter there, you will get something like this:



https://broadbandnow.com/Charter-Communications-speed-test

So in the real world of computer Internet users, you may be working with about ten percent of Spectrum's advertised speed. I could not care less about what the Millennial's are doing with their *dumb terminal* phones. (Cellular Newton's)

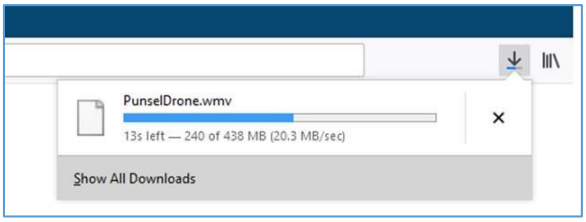
If you recall this, all started for me with an upgrade to what I thought (and you promised) was a faster service, because my streaming video would not consistently provide HD quality, and I wanted to use a VPN and Tor to research and write a book. It continued with me buying a new router to replace what the technicians called the "stuck" one that I had. Come to find out that neither the service upgrade nor the router improved my speed. It continued with me pounding Spectrum with emails, stories, lyrics, a song, and data for four months, five site visits by 8 technicians, currently ending up at the VP level and with a conversation with a Network Engineer.

So your VP offers platitudes like they only say "UP TO" 400Mbps speed, and that I should connect to their modem rather than my router for testing, which is where we started with all of this almost many months ago. Yet you use this same router to pronounce your system OK.

You network engineer can only offer even more platitudes like making sure no one else in our two person senior citizen house is using the Internet while I am testing or downloading. Or offering that if I am getting 160Mbps to my

website (less than half of advertised) it is truly remarkable considering that he and I started at 2400bps thirty years ago. I personally think that what really ***is*** remarkable and more useful is my computers going from a 4 MHz to a 4 GHz processor in that same time frame. This network engineer also tried to distract and appease me by letting me know that his own Comcast 600Mbps service tests out at around 300Mbps at most and he cannot reliably play streaming Disney movies, which need a whopping 6Mbps, during weekends and evenings.

So the message given here is be grateful for what you have, it could be worse, and we will cut your monthly price in half to reflect the half our promise you are actually getting. This pretty much confirms that my data is correct.



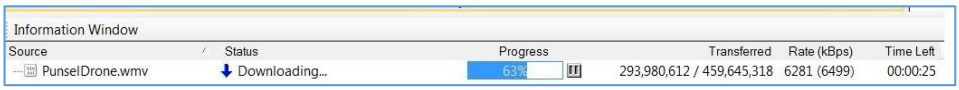
Firefox 88.0 HTTPS 162.4Mbps

For the sake of fairness, here are some examples of some contradictory quotes from other ISP's:

Answer One: "you're not rate limited etc….any speed issues are on your end (sorry)"

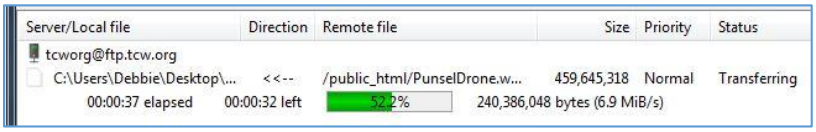
Answer Two: "We have software on the hosting servers so one customer cannot use up all of the resources and hurt other customers."

Answer One: "I'm sorry, but you're just not going to see the same speeds from the web server that you'll see from the speed test. The web server is not optimized for downloading files of the size of your movie as that's not the typical use case for clients." "If there was a problem with the server or our network we would have thousands of customers complaining about speed issues."



WS_FTP 6.5Mbps

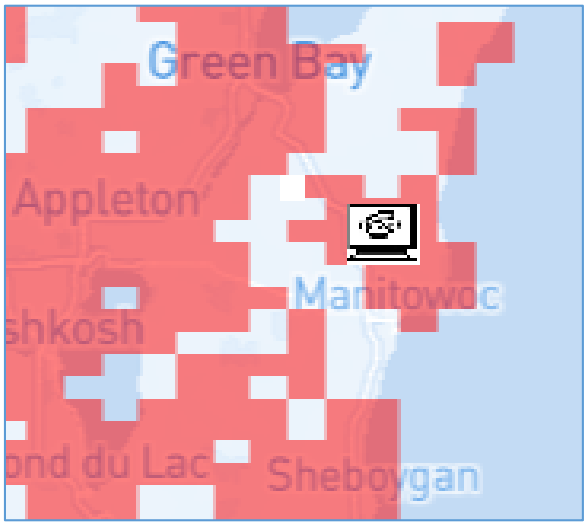
Answer Two: "All we have to go off of is from my desk the speeds are 600-900Mbps for FTP uploads/downloads and we are not hearing complaints from other customers."



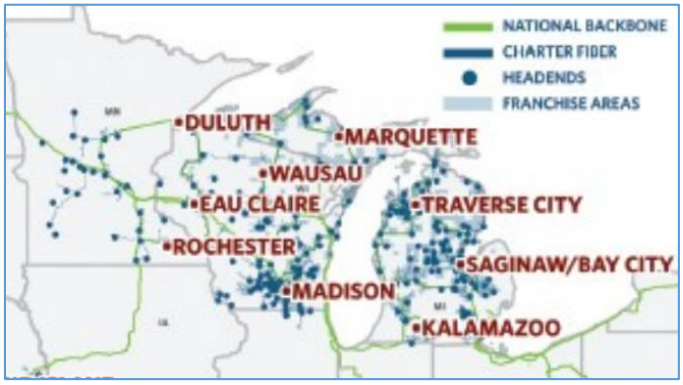
FTP FileZilla 58Mbp

Your VP says that Spectrum cannot control my speed ON the Internet, and I agree, but you CAN via your routing and peering arrangements control my speed TO the Internet.

After all, I am not paying you for super-fast access 100 miles or even 200 miles away. I have no business to those places.



What I am paying for is fast access to my website 100 miles south to my Franklin/Milwaukee website and TO the Global Internet 200 miles south at the Chicago IXP, neither of which I currently have. Nor do I have direct access 100 miles south to the Milwaukee IXP, 150 miles southwest to the Madison IXP, or 300 miles northwest to the Minneapolis IXP.



I appear to be on a bit of a red low bandwidth island here, and I am not sure where the portage to the backbone is.

https://broadbandnow.com/Charter-Communications/telecomramblings.com

Internet Transit

Since the Internet is a network of networks, to be connected to the Internet, any entity must attach itself to another entity that is already connected to the Internet. This is usually accomplished by purchasing a service called "Internet Transit." Internet Transit is the business relationship whereby an Internet Service Provider or ISP, sells access to the global Internet. Internet Transit is often a large component of the cost of operating an Internet service.

Think of the vast U.S. interconnected highway systems of Interstate, State, County, and Town roads that connect cities large and small across the United States. That complexity is similar to the information highway that makes up the backbone of the Internet (Interstate), except that instead of the government owning all of it, many entities do and are left to sort out all of the rules of these connections. These entities are called Internet service providers or ISP's.

This type of multi-faceted shared system means negotiation is key. These ISPs organize themselves into Tiers. Each tier corresponds to the level of IP Network Access.

The U.S. Internet Region Tier 1 ISPs

1. AT&T
2. Verizon
3. Sprint (Softbank Broadband)

4. Century Link (Qwest)
5. Level 3 (Global Crossing)
6. NTT/Verio

Upper Midwest six Tier 1 ISP's (1 of 8 US interconnect regions)

A Tier 2 network is an Internet service provider that engages in the practice of peering with other networks, but which also purchases IP transit to reach some portion of the Internet. Tier 2 providers are the most common Internet service providers, as it is much easier to purchase transit from a Tier 1 network than to peer with them and attempt to become a Tier 1 carrier.

Tier-2 Carriers include:

- Comcast
- Cox Communications
- CTS Telecom
- Charter Communications/Spectrum

Tier 3 is used to describe networks who solely purchase IP transit from other networks to reach the Internet.

Wisconsin Tier-3 carriers include:

- Cyberlynk
- Frontier Communications DSL/fiber (leased Verizon and AT&T lines)
- TDS Telecom DSL/fiber (leased AT&T lines)
- HierComm Networks, LLC (wireless broadband)
- Netwurx (wireless broadband)

When you hear talk about net neutrality, this is why. Tier-3 carriers are usually last mile providers, meaning they connect consumers to the Internet without a network of their own, servicing only the connection leading into your home or office. Content providers have little control over this part. As such, tier 3 ISP networks can be artificial congested, poorly maintained, or throttled.

Peering Agreements

Peering provides a more direct traffic path between the parties while reducing the load on these expensive transit services. Since peering is a nontransitive relationship, Internet Peering is not a perfect substitute for Internet Transit.

Internet Transit is a service that provides access to the global Internet, while Internet Peering simply provides a more direct path for a subset of the traffic.

Internet Peering is typically settlement-free, with each side deriving about the same value from the reciprocal arrangement. If either party perceives that the benefit derived from peering is asymmetric, one party or the other may deny peering or suggest an alternative paid arrangement.

If the cost of exchanging traffic in peering relationships is less than the cost of sending that traffic through a transit service, then peering can be a financially rational decision. Peering makes sense when it is cheaper to send traffic to peers than though a transit provider. *This is also, where the quality of the service provided (QOS) could degrade due to cost concerns and prioritization of convenience over performance.*

Transit usually provides a more circuitous path than peering – a path through potentially many networks. It is not uncommon to find more than 30 router hops from eyeballs to content.

However, the primary motivation for these ISPs is to own the home market and not make it easy for other ISP's to build in to their home market and compete with them.

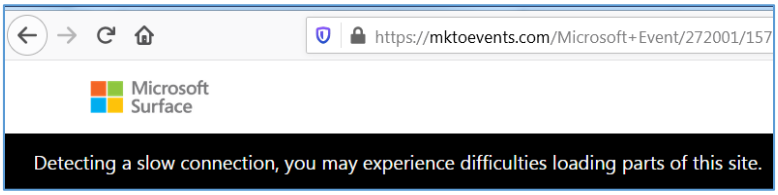
The cost of peering at an IXP usually involves: Transport fees (unmetered) for getting the traffic to the exchange point (IXP), Colocation fees, Equipment expenses plus the Peering port fees on the exchange point shared fabric.

References: *The 2014 Internet Peering Playbook: Connecting to the Core of the Internet © 2014 by William B. Norton and published by DrPeering Press*

https://www.ctstelecom.com/the-three-tiers-of-isps-what-they-mean-why-theyre-important/

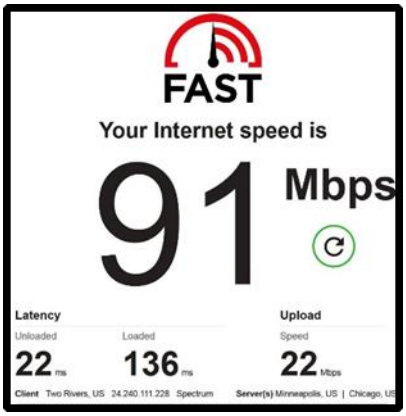
https://drpeering.net/FAQ/Who-are-the-Tier-1-ISPs.php

This is not something I like to see too often, but this is my real world.



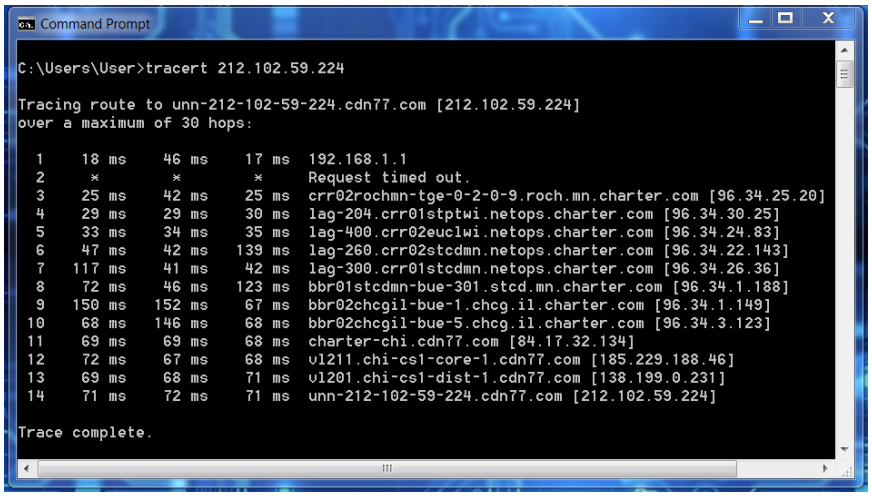
I continue to get video and audio stuttering on Amazon Prime Video that uses 15.2Mbps in Best video quality mode.

And this from Netflix:



I just want Spectrum to get me from their Tier 2 Intranet to the Intestate/Internet backbone where the speed limit of my vehicle/packets is 55Mph or in this case 400Mbps. Imagine our highway system being setup where the further you get from home the lower the speed limit drops. This is what I, and an unknown number of NE Wisconsin Spectrum customers have now.

If I connect to one of the Spectrum **Intranet** *beauty contest* speed test sites, I can get a speed reading of 459Mbps. If I then turn on a software VPN and go to the same site via a VPN server residing on the **Chicago Internet backbone***, I get a reading of 129Mbps. This is speed drop is not fully a result of the VPN encryption overhead, nor the speed or bandwidth of the VPN server, but is mostly related (see spreadsheet data) to connecting to this test site via the Internet rather than the Spectrum *Intranet*.



** DataCamp Limited, in Chicago with a 30Tbps plus Global Network.*

I do not know exactly how or where I get to the Internet backbone, so I cannot do a speed test to that point.

What this means in real life terms is that I get poor download and upload speeds to my web hosting site, to the Internet in general, and I cannot decently run a VPN. This is because I do not really have an Internet backbone connection, but rather a Spectrum **Intranet** connection that eventually meanders around and connects to the Internet somewhere and somehow. This also means me not being able to consistently stream HD movies from Netflix and Prime Video.

So in the end, Internet access is not about Spectrum Internet Ultra's speed to a *beauty contest* test site. It is really about how much of the Internet bandwidth Spectrum will allow me to have access to. They are the gatekeepers who determine how much bandwidth (and perhaps content) of this public utility, I am allowed to access. This seems to be directly at odds with the way our public utilities governed by the Wisconsin Public Service Commission or PSC generally operate.

PS. Oh, and now you are helping to break it…for your profits.

> *By* David McCabe *The New York Times*
> *May 6, 2021Updated 1:58 p.m. ET*
> *Internet service providers funded an effort that yielded millions of fake comments supporting the Federal Communications Commission's repeal of so-called* net neutrality *rules in 2017, the New York attorney general said on Thursday.*
> *Internet providers, working through a group called Broadband for America, spent $4.2 million on the project, the attorney general said. The effort generated roughly nine million comments to the agency and letters to Congress backing the rollback, almost all of which were signed by people who had never agreed to the use of their names on such comments, according to the investigation. Some of the names had instead been obtained earlier, in other marketing efforts, and were then used to submit comments, officials said. The agency approved the repeal in late 2017.*
> *Broadband for America's members include some of America's most prominent Internet providers, like AT&T, Comcast and* ***Charter****, as well as several trade groups representing the industry.*
> *Broadband for America, AT&T, Charter, and Comcast did not immediately respond to requests for comment.*

https://www.nytimes.com/2021/05/06/technology/Internet-providers-fake-comments-net-neutrality-new-york.html?link_id=5&can_id=fc43a50924502a3e547a3ad5d166f0f6&source=email-breaking-big-cables-fraudulent-comments-2&email_referrer=email_1167660&email_subject=fraud

PPS. This is as tone deaf, unethical, and immoral as Bezos building new twin yachts, while most people suffer because of the pandemic and unbridled capitalism. At the going rate of $50k per mile, your bosses' pay raise alone would bring fiber to my house and to 600 other people. It is funny how shareholder return on investment is a concern when investing in rural broadband, but not when it comes to CEO pay.

Charter CEO Tom Rutledge's Pay Rises to $38.8 Million in 2020

The exec's compensation at the U.S. cable and Internet giant rose sharply from $8.74 million in 2019.

https://www.hollywoodreporter.com/business/business-news/charter-ceo-tom-rutledges-pay-rises-to-38-8-million-in-2020-4146926/

So in the end after projecting more than ten thousand words, graphics, test data, and humorous (to me) song lyrics at Spectrum, I have a minor improvement in speed at a reduced cost for three years. Maybe, given that time they can fix their network. Or perhaps they will merge with another bad company.

A pyrrhic **victory** at best, me thinks.
And sometimes, just occasionally the good guys win one or two.

Cable Giants, ISPs, Telcos End Legal Fight Against California's Net Neutrality Law (theregister.com) 11

Posted by BeauHD on Friday May 06, 2022 @06:02PM from the case-closed dept.

An anonymous reader quotes a report from The Register: California Attorney General Rob Bonta on Wednesday welcomed the decision by a group of telecom and cable industry associations to abandon their legal challenge of the US state's net neutrality law SB822. "My office has fought for years to ensure that internet service providers can't interfere with or limit what Californians do online," said Bonta in a statement. "Now the case is finally over. Following multiple defeats in court, internet service providers have abandoned this effort to block enforcement of California's net neutrality law. With this victory, we've secured a free and open internet for California's 40 million residents once and for all."

In December 2017, then Federal Communications Commission (FCC) chair Ajit Pai tossed out the 2015 net neutrality rules put in place during the Obama administration, freeing broadband providers to block, throttle, and prioritize internet traffic, among other things -- all of which were disallowed under the 2015 rules. On September 30, 2018, then California Governor Jerry Brown signed into law Senate Bill 822 (SB822), which more or less restored those rules. That same day, the Justice Department under the Trump administration challenged the law, as subsequently did the broadband companies benefiting from what Pai at the time referred to as a "light-touch approach."

The Justice Department, under the Biden administration, ended its opposition to California's net neutrality law back in February, 2021. The industry plaintiffs continued fighting SB822 in court but faced a setback in January, 2022, when the US Court of Appeals for the Ninth Circuit refused to block the law's enforcement as litigation progressed. Now those groups -- ACA Connects

(America's Communications Association), CTIA (The Wireless Association), NCTA (The Internet & Television Association), and USTelecom (The Broadband Association) -- have withdrawn too. The trade associations, with the agreement of Bonta, filed a joint stipulation of dismissal without prejudice which ends the telco legal challenge but allows the claim to be refiled at some later date.

Frontier Lied About Internet Speeds and 'Ripped Off Customers', FTC Says (arstechnica.com) 18

Posted by msmash on Friday May 06, 2022 @04:45PM from the time-to-face-the-music dept.

The Federal Trade Commission today said it "has moved to stop Internet service provider Frontier Communications from lying to consumers and charging them for high-speed Internet speeds it fails to deliver." From a report: Frontier was sued by the FTC in May 2021, and on Thursday, it agreed to a settlement with the FTC and district attorneys in Los Angeles County and Riverside County who represented the people of California. Frontier must pay $8.5 million to California "for investigation and litigation costs" and another $250,000 that will be distributed to Frontier customers who were harmed by Frontier's alleged actions. Frontier must also make changes, such as letting customers cancel service at no charge and "discounting the bills of California customers who have not been notified that they are receiving DSL service that is much slower than the highest advertised speed," the FTC said.

Charter/Spectrum Wisconsin IP assignments

IP ADDRESS NETBLOCKS

Charter Communications CHTR-HSA-2BLK (NET-24-240-0-0-1) 24.240.0.0 - 24.241.255.255

24.240.2.0-255 - Watertown, WI
24.240.3.0-255 - Watertown, WI
24.240.4.0-255 - Delavan, WI
24.240.5.0-127 - Delavan, WI
24.240.5.128-255 Elkhorn, WI
24.240.6.0-255 - Delavan, WI
24.240.7.0-255 - Delavan, WI

24.240.10.128-191 - Wautoma, WI
24.240.10.192-199 - Neshkoro, WI
24.240.10.200-209 - Wautoma, WI
24.240.10.210-228 - Adams, WI
24.240.10.229-255 - Redgranite, WI
24.240.11.0-255 - Mankato, MN
24.240.12.0-255 - Genoa City, WI
24.240.13.0-255 -Twin Lakes, WI
24.240.14.0-255 - Beaver Dam, WI
24.240.15.0-255 - Chippewa Falls, WI

24.240.32.0-255 - Madison, WI
24.240.33.0-255 - Madison, WI
24.240.34.0-255 - Madison, WI
24.240.35.0-255 - Madison, WI
24.240.36.0-255 - Madison, WI
24.240.37.0-255 - Madison, WI
24.240.38.0-255 - Madison, WI
24.240.39.0-255 - Madison, WI
24.240.40.0-255 - Madison, WI
24.240.41.0-255 - Madison, WI
24.240.42.0-255 - Madison, WI
24.240.43.0-255 - Madison, WI
24.240.44.0-255 - Madison, WI
24.240.45.0-255 - Oregon, WI

24.240.47.0-255 - Janesville, WI
24.240.48.0-255 - Madison, WI
24.240.49.0-255 - Madison, WI

24.240.50.0-127 - Whitewater, WI
24.240.50.128-255 - Janesville, WI
24.240.51.0-255 - Whitewater, WI
24.240.52.0-255 - Eau Claire, WI
24.240.53.0-255 - Eau Claire, WI
24.240.54.0-255 - Eau Claire, WI
24.240.55.0-255 - Eau Claire, WI
24.240.56.0-255 - Wausau, WI
24.240.57.0-255 - Wausau, WI
24.240.58.0-255 - Fond du Lac, WI
24.240.59.0-255 - Fond du Lac, WI
24.240.60.0-255 - Janesville, WI
24.240.61.0-255 - Janesville, WI
24.240.62.0-255 - Sturgeon Bay, WI
24.240.63.0-255 - Sturgeon Bay, WI
24.240.64.0-255 - Janesville, WI
24.240.65.0-255 - Janesville, WI

24.240.68.0-255 - Delevan, WI
24.240.69.0-255 - Delevan, WI
24.240.70.0-127 - Rhinelander, WI
24.240.70.128-255 - Fond du Lac, WI

24.240.74.0-255 - Madison, WI
24.240.75.0-255 - Madison, WI
24.240.76.0-255 - Superior, WI
24.240.77.0-255 - Superior, WI

24.240.80.0-255 - Janesville, WI
24.240.81.0-255 - Janesville, WI
24.240.82.0-63 - Janesville, WI
24.240.82.64-127 - Edgerton, WI
24.240.82.128-223 - Janesville, WI
24.240.82.224-239 - Evansville, WI
24.240.82.240-255 - Fort Atkinson, WI
24.240.83.0-127 - Janesville, WI
24.240.83.128-159 - Lake Mills, WI
24.240.83.160-238 - Janesville, WI
24.240.83.239-255 - Edgerton, WI
24.240.84.0-255 - Stevens Point, WI
24.240.85.0-255 - Stevens Point, WI
24.240.86.0-255 - Sun Prairie, WI
24.240.87.0-255 - Lodi, WI

24.240.88.0-255 - Madison, WI
24.240.89.0-255 - Madison, WI

24.240.92.0-255 - Janesville, WI
24.240.93.0-255 - Janesville, WI
24.240.94.0-255 - Janesville, WI

24.240.112.0-255 - Sun Prairie, WI
24.240.113.0-255 - Sun Prairie, WI
24.240.114.0-255 - Madison, WI
24.240.115.0-255 - Madison, WI
24.240.116.0-255 - Wausau, WI
24.240.117.0-255 - Schofield, WI
24.240.118.0-255 - Sun Prairie, WI
24.240.119.0-255 - Sun Prairie, WI
24.240.120.0-15 - Fitchburg, WI
24.240.120.16-31 - Milton, WI
24.240.120.32-47 - Madison, WI
24.240.120.48-63 - Waunakee, WI
24.240.120.64-79 - Eau Claire, WI
24.240.120.80-95 - Beaver Dam, WI
24.240.120.96-111 - Rhinelander, WI
24.240.120.112-127 - Rhinelander, WI
24.240.120.128-143 - Sun Prairie, WI
24.240.120.144-159 - Houghton, MI
24.240.120.160-175 - Beaver Dam, WI
24.240.120.176-191 - Rice Lake, WI

24.240.120.208-223 - Rhinelander, WI
24.240.120.224-239 - Janesville, WI
24.240.120.240-255 - Milton, WI
24.240.121.0-15 - Wausau, WI
24.240.121.16-31 - Rhinelander, WI
24.240.121.32-47 - Beaver Dam, WI
24.240.121.48-63 - Wausau, WI
24.240.121.64-79 - Beloit, WI
24.240.121.80-111 - Madison, WI
24.240.121.112-143 - Onalaska, WI
24.240.121.144-159 - Milton, WI
24.240.121.160-175 - Juneau, WI
24.240.121.176-191 - Iron Mountain, MI
24.240.121.192-207 - Beloit, WI
24.240.121.208-223 - Tomah, WI

24.240.121.224-239 - Madison, WI
24.240.121.240-255 - Beloit, WI
24.240.122.0-15 - Waunakee, WI
24.240.122.16-47 - Madison, WI
24.240.122.48-63 - New Holstein, WI
24.240.122.64-79 - Fond du Lac, WI
24.240.122.80-95 - Wausau, WI
24.240.122.96-111 - Madison, WI
24.240.122.112-127 - Sheboygan, WI
24.240.122.128-143 - Madison, WI
24.240.122.144-151 - Wisconsin Rapids, WI
24.240.122.152-159 - Fond du Lac, WI
24.240.122.160-175 - Fitchburg, WI
24.240.122.176-179 - Waupaca, WI
24.240.122.180-183 - Eau Claire, WI
24.240.122.184-191 - Fitchburg, WI
24.240.122.192-207 - Madison, WI
24.240.122.208-223 - Iron Mountain, MI
24.240.122.224-239 - Waupaca, WI
24.240.122.240-255 - Portage, WI
24.240.123.0-15 - Eau Claire, WI
24.240.123.16-31 - Madison, WI
24.240.123.32-63 - West Bend, WI
24.240.123.64-95 - Rothschild, WI
24.240.123.96-111 - Wausau, WI
24.240.123.112-127 - Rothschild, WI
24.240.123.128-143 - Eau Claire, WI
24.240.123.144-159 - Watertown, WI
24.240.123.160-175 - Wausau, WI
24.240.123.176-191 - Waupaca, WI
24.240.123.192-207 - Lake Mills, WI
24.240.123.208-223 - Kewaskum, WI
24.240.123.224-239 - West Bend, WI
24.240.123.240-255 - Madison, WI

How we got to where we are

BBS or Bulletin Board Systems

The invention of Bulletin Board Systems (BBS) in 1978 was the beginnings of the public online world.[28] Computer users could connect via a phone line and modem to upload and download software and data, read news and bulletins, play online games, and exchange messages with other users through public message boards and sometimes via direct chatting in chat rooms. In the early 1990's there were as many as 60,000 BBSes in the US. For about 20 years, BBSes were the best way to go online.[29]

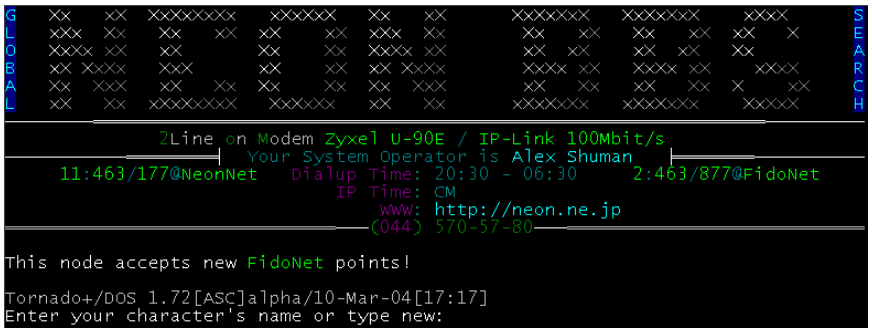


Image courtesy of Wikipedia.org

These BBSes used a rather primitive text based terminal user interface (TUI).

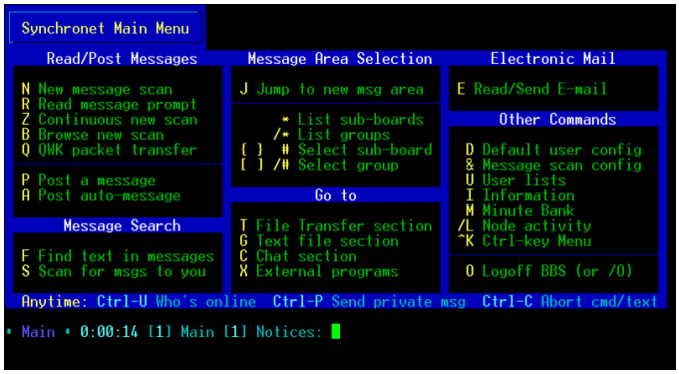


Image courtesy of Wikipedia.org

---

[28] *A bulletin board system or BBS is a computer server running software that allows users to connect to the system using a computer terminal program.*

[29] *For a five hour video history of the BBS, visit:*

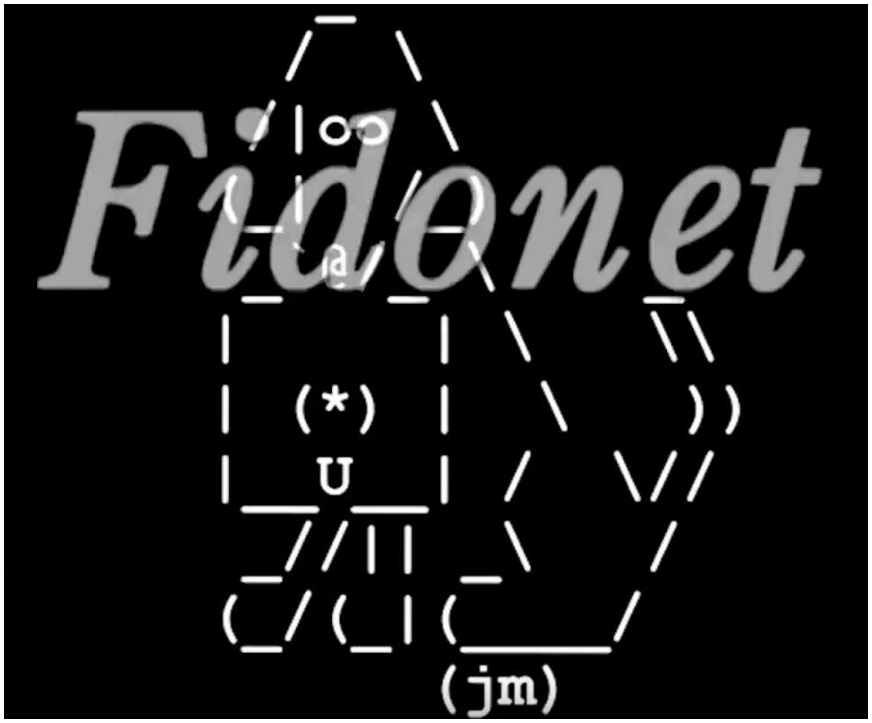
https://www.youtube.com/watch?v=nO5vjmDFZaI

FidoNet

FidoNet was a worldwide computer network that was used for communication between bulletin board systems (BBSes). It used a store-and-forward system[30] to exchange private (email) and public (forum) messages between the BBSes in the network, as well as other files and protocols in some cases. It effectively networked all the BBSes together. An Internet of BBSes effectively, which eventually exceeded 35,000 nodes.

The system was highly efficient; using the latest file compression and file transfer systems to aggressively drive down the cost of transmission on what was largely at that time a hobby network.

The practical implications of this was the you could now download files and send emails anywhere around the world, by just making a local call to a BBS.



[30] Store and forward is a telecommunications technique in which information is sent to an intermediate station where it is kept and sent at a later time to the final destination or to another intermediate station. The intermediate station, or node in a networking context, verifies the integrity of the message before forwarding it.

Gopher

In the early days of the Internet, things were a bit primitive.

The Gopher protocol is a TCP/IP protocol designed for distributing, searching, and retrieving documents over the Internet. The Gopher protocol was strongly oriented towards a menu-document design but ultimately Hypertext Transfer Protocol (HTTP) became the dominant protocol. The Gopher ecosystem is often regarded as the effective predecessor of the World Wide Web. Gopher's hierarchical structure provided a platform for the first large-scale electronic library connections.

Image courtesy of Wikipedia

Archie was a tool for indexing FTP archives, allowing people to find specific files. It is considered to be the first Internet search engine.

Veronica was a search engine system for the Gopher protocol. During its existence, Veronica was a constantly updated database of the names of almost every menu item on thousands of Gopher servers. The Veronica database could be searched from most major Gopher menus.

Jughead was a search engine system for the Gopher protocol. It was distinct from Veronica in that it searched a single server at a time.

Usenet

Usenet in 1979–80, introduced a new generation to life online, unlike the cloistered ARPANET,

Around the same time that the BBS was invented, two academics at Duke University set themselves an even more ambitious task. Tom Truscott and Jim Ellis were aggrieved that the ARPANET was elite and expensive and cost approximately $100,000 per year. In 1979 they set up a network called “Usenet,” which, anyone could access and use. (Anyone of a very few people at the time that is, who had a computer connected to the operating system UNIX.)

Usenet was a worldwide-distributed discussion system available on computers. It was developed from the general-purpose Unix-to-Unix Copy (UUCP) dial-up network architecture. Users read and post messages (called articles or posts, and collectively termed news) to one or more categories, known as newsgroups. Usenet resembles a BBS in many respects and is the precursor to Internet forums that are used today. Discussions are threaded, as with web forums and BBSs, though posts are stored on the server sequentially. The name comes from the term "user’s network.”

One notable difference between a BBS or web forum and Usenet is the absence of a central server and dedicated administrator. Usenet is distributed among a large, constantly changing conglomeration of servers that store and forward messages to one another in so-called news feeds. Individual users may read messages from and post messages to a local server operated by a commercial Usenet provider, their Internet service provider, university, employer, or their own server.

Usenet has significant cultural importance in the networked world, having given rise to, or popularized, widely recognized concepts and terms such as "FAQ,” "flame,” and "spam.”

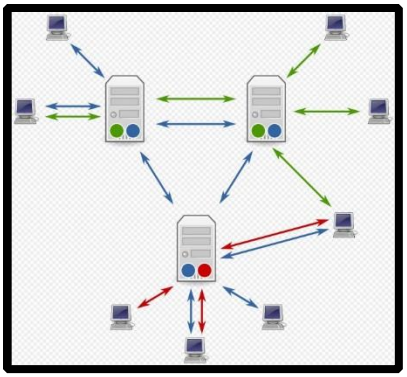


Image courtesy of Benjamin D. Esham

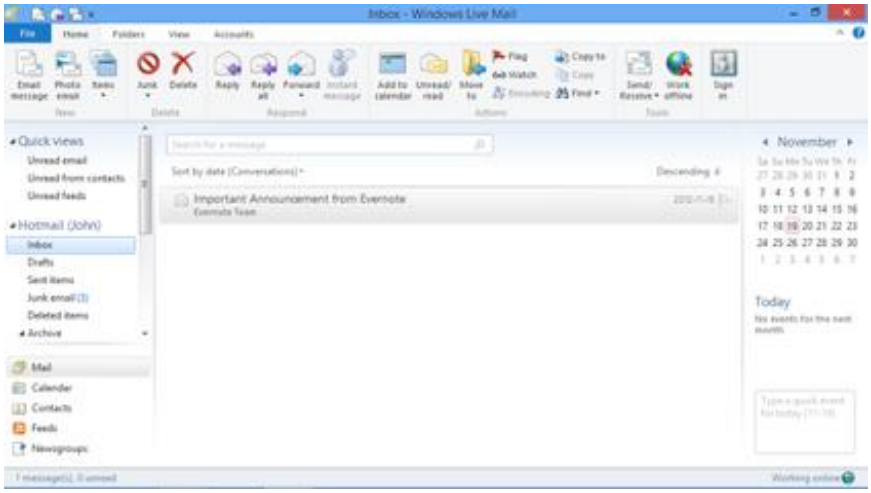
In the diagram above of Usenet servers and clients, the blue, green, and red dots on the servers represent the groups they carry. Arrows between servers indicate newsgroup group exchanges (feeds). Arrows between clients and servers indicate that a user is subscribed to a certain group and reads or submits articles.

A Usenet newsgroup is a repository usually within the Usenet system, for messages posted from many users in different locations using Internet. (Despite the name, newsgroups are discussion groups. They are not devoted to publishing news, although this had been intention when the Internet was young. Newsgroups are technically distinct from, but functionally similar to, discussion forums on the World Wide Web. Newsreader software, i.e. MS Outlook Express, was used to read the content of newsgroups.

Before the adoption of the World Wide Web, Usenet newsgroups were among the most popular Internet services, and have retained their noncommercial nature in contrast to the increasingly ad-laden web. In recent years, this form of open discussion on the Internet has lost considerable ground to individually operated browser-accessible forums and big media social networks such as Facebook and Twitter.

Newsgroups

Programs called newsreaders are used to read and post messages (called articles or posts, and collectively termed news) to one or more newsgroups. Most email readers are also newsreaders, as in the case of the former email software included with MS Windows called MS Outlook Express.



By Source, Fair use, https://en.wikipedia.org/w/index.php?curid=22357104

The current day web is overrun with junk. Between the pop-ups, the auto playing videos, the cookie banners, the incessant calls for sign-ups, the coupon offers, the "Don't forget to subscribe!" reminders, the in-line ads slowing the page down, the slew of trackers also slowing the page down. For lots of reasons, some good and some bad, much of the Internet has become totally unusable.

Now some are thinking that we should go back to the future:

https://plaintextsports.com/

CompuServe, Prodigy, and AOL

These early BBS's were followed by more advanced features and interfaces of CompuServe, Prodigy, and AOL.

Some of the resources and services which online services have provided access to, included message boards, chat services, electronic mail, file archives, current news and weather, online encyclopedias, airline reservations, and online games. Major online service providers like CompuServe also served as a way for software and hardware manufacturers to provide online support for their products via forums and file download areas within the online service provider's network.

Image courtesy of Wikipedia.org

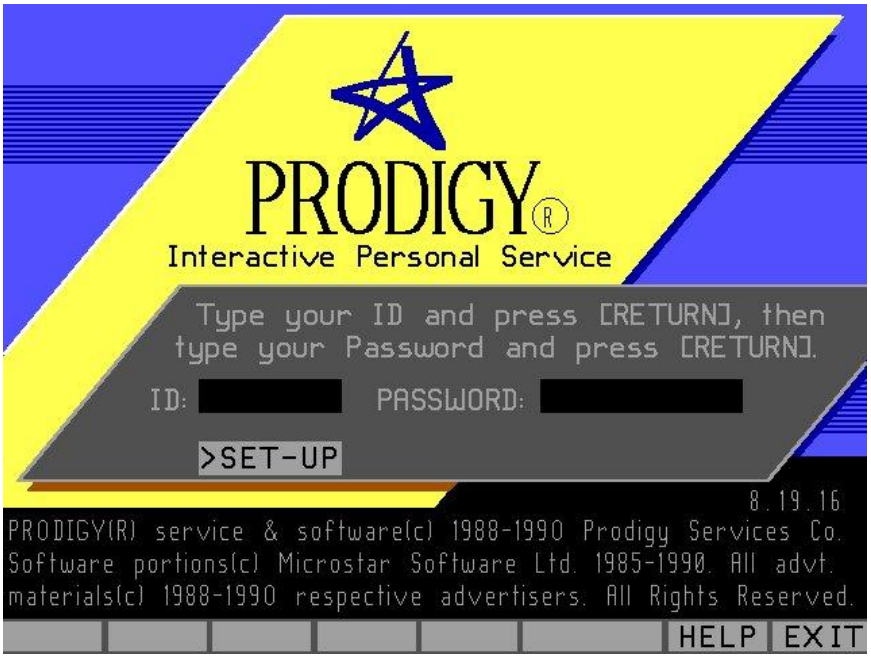


Image courtesy of Wikipedia.org

Image courtesy of Wikipedia.org

The Emergence Of The Internet and the Web

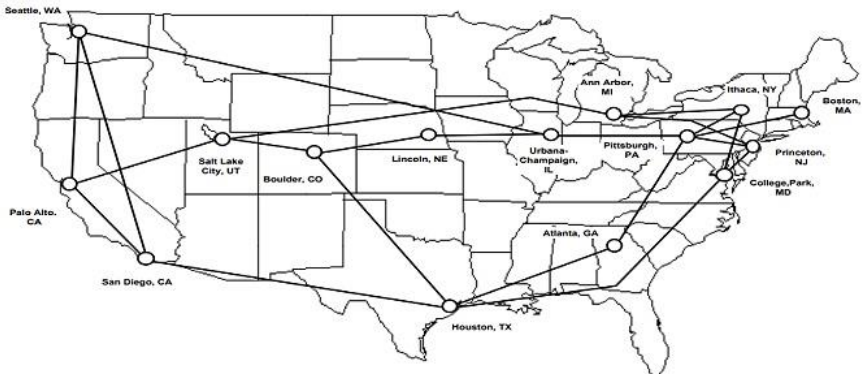
Once the Internet became open to the public, the walled gardens of AOL, Prodigy, and CompuServe were beginning to be seen by its users as too restrictive. While these services now added an onramp to the Internet from their services, users who discovered the Mosaic browser, later Netscape, and even later Microsoft's Internet Explorer browser (in the Windows 95 Plus Pack) found a more direct and less expensive path.

Reinforcing the idea that timing is everything, Microsoft introduced a walled garden network called the MSN right at the time users were escaping them. Windows 95 beta testers were given free access to this service for one year. This service was very professional looking with innovative content with an onramp to the Internet as well. The slow performance of the graphic intensive interface however exceeded what most 28.8 kbps modem users at the time would have the patience for.

Microsoft would misjudge the level of bandwidth available to users outside of Seattle and would make this mistake again later by removing optical drive support in Windows too soon.

The brief back story on the formation of the Internet is that by 1985 the National Science foundation formed the NSFNET, linking five supercomputer centers at Princeton University, Pittsburgh, University of California at San Diego, University of Illinois at Urbana-Champaign, and Cornell University.

The NSFNET begat the ARPANET which begat the DARPANET which begat the Internet.



1994 Internet backbone

A very good journalistic history of the Internet is here:

https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/

The Internet then subsumed the Web, which we call the Clear Web today. A couple of excerpts from my book *The Insider (A Life Inside the Personal Computer)*

At around this same time Lefty ran into an old acquaintance from PARC, Bob Metcalfe, at one of the many computer shows which they both attended. Over lunch, Bob told him an old story from his MIT days and about the trials and tribulations of co-inventing Ethernet.[31]

"I came to work one day at MIT and the computer had been stolen so I called DEC to break the news to them that this $30,000 computer that they'd lent me was gone. They thought this was the greatest thing that ever happened because it turns out I had in my possession the first computer ever small enough to be stolen!"

Of course, Lefty told a story to Bob, which he had been told Vint Cerf.

In the World Wide Web's first generation, Tim Berners-Lee[32] launched the ideas of the URL, HTTP, and HTML. A few people noticed that the Web might be better than Gopher. In the second generation, Marc Andreessen and Eric Bina developed the NCSA Mosaic web browser at the University of Illinois. Several million people then suddenly noticed the Web might be better than sex. In the third generation, Andreessen and Bina left NCSA to found Netscape and gave the browser away free, and now hundreds of millions of people are using it and its descendants.

Marc Andreessen, born and raised in Lefty's home state of Wisconsin, received his bachelor's degree in Computer Science from the University of Illinois at Urbana-Champaign. He also worked at the National Center for Supercomputing Applications (NCSA) at the university, where he became familiar with Tim Berners-Lee's open standards for the World Wide Web. Andreessen and co-worker Eric Bina were working at the university under National Science Foundation or NSF funding, championed by then Senator Al Gore. They then created a user-friendly Internet web browser that worked on a wide range of computers. That computer code became the Mosaic Web browser, and the basic code for other browsers including the code licensed from Spyglass Mosaic for Internet Explorer.

When Lefty got him to talk about his work again, the British born Tim Berners-Lee explained that he had worked as an independent contractor at CERN for a half year around 1980. In 1984, he returned to CERN, this time as a fellow.

Tim continued his story, "They buy a very expensive NeXTcube computer for evaluation, and gave it to me to use. I did my prototype implementation of the web

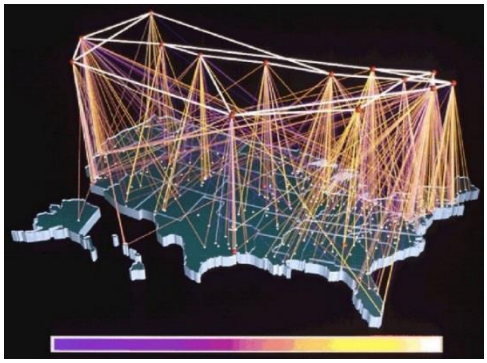
---

[31] *Ethernet is a computer networking technology used to connect computers to each other in local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs).*

[32] *Later on the 25th anniversary of the web Tim Berners Lee when questioned Edward Snowden, Hero or villain? Replied, "The whistleblower may be all that saves our society."*

using NeXTSTEP within a few months, thanks to the qualities of the NeXTSTEP software development system. This prototype offered WYSIWYG (What You See Is What You Get) browsing and authoring. During later brainstorming sessions in the CERN cafeteria, Tim and the group searched for a name, which remained unused from Greek mythology characters. I proposed 'World-Wide Web', and they all liked the name. The rest as they say is history."

CERN, then the largest Internet node in Europe, provided Berners-Lee with an opportunity to join his hypertext with the Internet. "I just needed to take the hypertext idea and connect this to the Transmission Control Protocol, TCP, and domain name system ideas and—ta-da!—the World Wide Web. The creation of the web came as an act of desperation, because the situation was otherwise difficult when I worked at CERN. Most of the technology involved within the web, hypertext, and multi-font text objects, had been designed already. I just needed to put them together. I took the step of first generalizing, and then going to a higher level of abstraction. This involved thinking about the documentation systems out there, as being possibly part of a larger imaginary documentation system."



"The goal of the Web is to serve humanity. We build it now so that those who come to it later will be able to create things that we cannot ourselves imagine." - Tim Berners-Lee

Note: WAIS was one of the first public search engines. Pervious search engines NASA RECON, Dialog, and OCLC, were private for a relatively narrow data set. WAIS made public Internet resources searchable. (Google's real ancestor).

So now, you know how we got to where we are; let us go off into this brave new world of the Deep and Dark Web.

But wait, there's more. Let us first expand on the current state of the Clear Web.

The Problems with the Clear Web

Pseudo Information Security

Here is another much shorter story:

Dear Bank,

So I watched this generic business focused security Webinar you kindly offered to me, and learned that the presenter, SBS Cybersecurity, is a firm that assists banks with audits, disaster responses etc. and bank employees with training and awareness etc. This probably checks a box on the banks regulatory requirements and so this is all good and well done as far as it goes.

While this might be great for the bank, I do not see a non-business bank customer focus. This is a missed opportunity to educate your non-business customers and to roll out 2FA across all your customer bank accounts, not just for business customers. Unsuspecting citizens is probably the area where the most need is, i.e. 66% are personal data hacks. This seminar was absent any discussion of https browser security, browser cookies, browser fingerprinting, search engine data harvesting (Chrome, Safari, Edge), which may lead to identity theft in the first place. Also absent was discussion of the downsides of cloud storage (single point of attack), the downsides of hacked password manager software, or any information regarding secure browsing, file encryption, email encryption, etc.

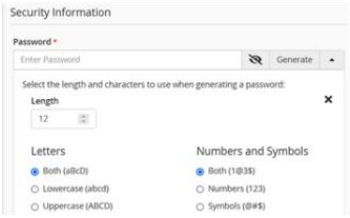
As for me, myself, I currently have 2FA on:

1. *Credit Union account (clear text SMS, kinda bad)*
2. *PayPal account (clear text SMS, kinda bad)*
3. *Amazon account (clear text SMS, kinda bad)*
4. *Account at your bank (token, kinda good but you made me change from a personal account to a business account and for me to be insistent to actually get that done)*

If you do not want to use kind of bad clear text SMS 2FA, or pass out tokens to everyone, you could use CAPTCHA like this for DDoS protection.

Our President requests Americans and corporations to tighten up Cyber Security because of Russia, China, North Korea, Iran, etc. (80% of critical infrastructure is privately held and not subject to government regulation) But the government does provide guidance and best practices and most certainly recommends multi-factor authentication.

https://www.cisa.gov/uscert/ncas/current-activity/2022/03/03/nsa-releases-network-infrastructure-security-guidance



So it is well past time for your bank and others to tighten up!

How about a secure password generator like in cPanel?

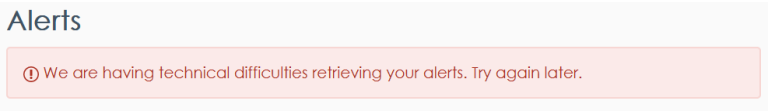
Btw, SBS CyberSecurity uses CAPTCHA to do something as simple as sending them an email from their website.

On the plus side, your bank rolling out account security alerts was a good thing.

You successfully accessed your online banking system on Apr 29, 2022.Your security is important to us. If you did not access your online banking system, please contact us immediately at [redacted]
Thank you for your business!
Sincerely,

A good first step, but now is the time to take the second step for competitive parity if not for an advantage for customer service.

Although this message is not helpful at all:



Convenience or security. You can pick only one.

Btw, it is not just about my account. Any hacked account can bring the bank down. DDoS AaaS hitting F5 (refresh page) hundreds of times per second.

Signed, your customer who is feeling a bit insecure

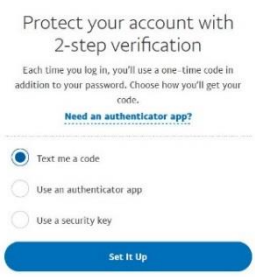
So the way that Internet security works on the Clear Web now is with encrypted transmission of text to and from websites using https. (Secure http SSL 2.0 and SSL 3.0) About 80% of sites now use this, up dramatically since the Snowden government spying revelations.

https://w3techs.com/technologies/details/ce-httpsdefault

If you login to Amazon.com to make a purchase (or watch a movie) if you have 2FA[33] turned on you will be presented with an account login for email and an additional similar looking dialog box for your password.

With 2FA on you will also be prompted for an OTP (one time password) that can be delivered to your phone via a clear text SMS[34] message. (What the kids call a text these days)

Once entered the system will log you into the site.



Turning on 2FA in PayPal.

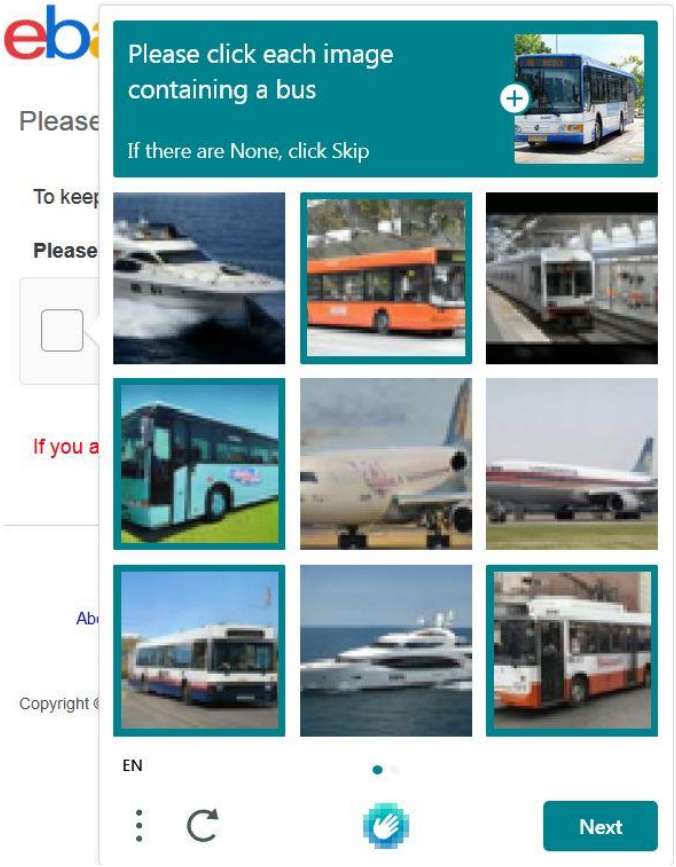
[33] *2FA,is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.*

[34] *SMS (Short Message Service) is a text messaging service. The first test SMS message was sent on December 3, 1992 from and to a computer.*

If you login to PayPal to pay for an eBay purchase or send or receive money, with 2FA you will be presented with a CAPTCHA (Turing Test) to prove you are not a bot. (computer robot)

Checking the box gives you another dialog box to send you an SMS code if that is the method you selected.

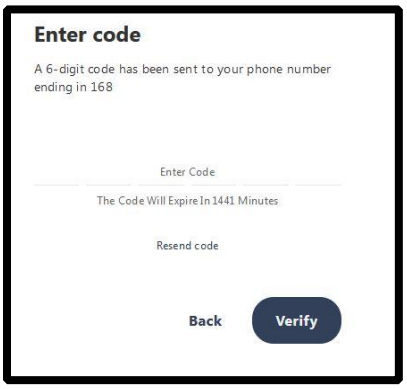
eBay CAPTCHA



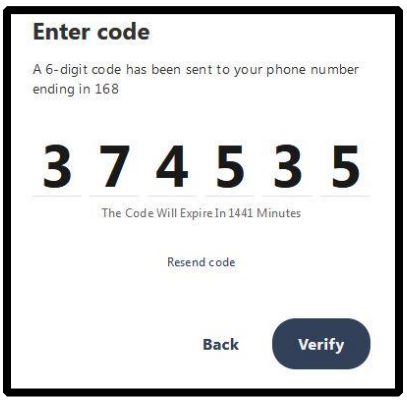
Amazon CAPTCHA

Some banks and credit unions who offer 2FA will provide you with something similar to this after the normal username and password login:

Clear text SMS, an unencrypted email, or a recorded phone call.



It will prompt you for the code you received from whatever method you choose.

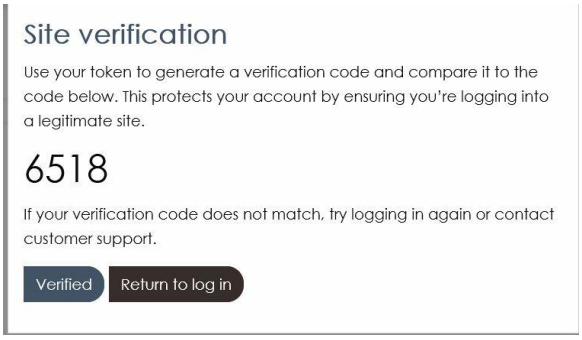


This code is good for 1441 minutes (24 hours, plenty of time for the bad guys to hack it) When you enter this code you will be logged into your accounts.

Some banks, will offer hardware tokens to business accounts and sometimes with persuasion, for retail customer accounts.

Into the usual login dialog box, you enter your username and for the password you enter your hardware token display readout followed by your security code. (8+4 digits)

You will then be presented with a second verification dialog box, and if it agrees with the second readout on your hardware token display, and you click on the verified button, you are logged in to the site.



These hardware tokens are very low cost (about twelve bucks on Amazon) or available from your bank at no cost and are easy to use.

Additional info in hardware tokens.

- https://vip.symantec.com/
- https://www.onespan.com/topics/bank-tokens
- https://www.peerspot.com/products/comparisons/-onespan-digipass_vs_symantec-vip-access-manager
- https://www.gartner.com/reviews/market/user-authentication/compare/broadcom-symantec-vs-onespan
- https://www.zdnet.com/article/best-security-key/

Black Hat Hackers want your data too.

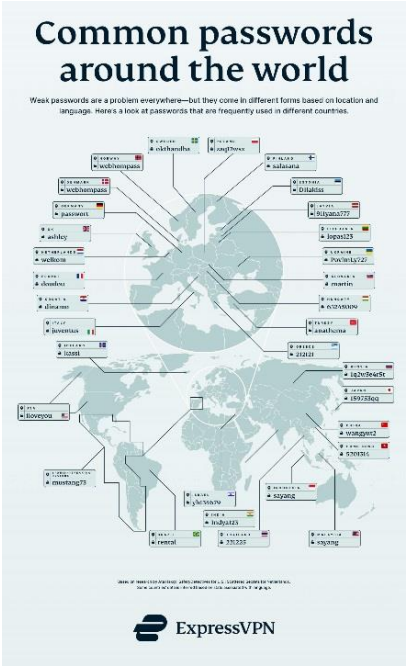
On the security side, the primary protocol all Web browsers currently use to encrypt their connections to websites, Transport Layer Security (TLS), can be attacked via traffic analysis to reveal the contents of encrypted communications. The analysis of network traffic metadata can also reveal the content of encrypted Domain Name. System (DNS) queries in protocols such as DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH). The Internet was simply not designed with privacy as a fundamental property at its inception, and today we are living with the consequences of those design choices.

In addition to acting as a side channel that may reveal encrypted content, the network-level metadata associated to online activities can be exploited to uniquely identify users, enable pervasive tracking, and reveal private information about personal or business activities. By applying "artificial intelligence" algorithms to this metadata, it is possible to predict people's political preferences, associations, social relations, purchasing behavior and other intimate details of their private lives and minds. In addition to the current widespread corporate exploitation of metadata for advertising and sales purposes, there is evidence of metadata collection and analysis being carried out en masse by the US National Security Agency (NSA) and similar agencies around the world.

The Problems with Passwords

200 worst passwords for 2020

https://nordpass.com/json-data/top-worst-passwords/pdfs/worst-passwords-2020.pdf



https://www.expressvpn.com/blog/infographic-common-passwords-by-country/?utm_campaign=blog_20220503_passwords&utm_content&utm_medium=apps&utm_source=rotating_message

For user authentication, passwords are stored either as plaintext or hashes. Since passwords stored as plaintext are easily stolen if database access is compromised, databases typically store hashes instead. Thus, no one – including the authentication system – can learn a password merely by looking at the value stored in the database.
When a user enters a password for authentication, a hash is computed for it and then compared to the stored hash for that user. Authentication fails if the two hashes do not match.;
To learn a password from a hash is to find a string which, when input into the hash function, creates that same hash. This is the same as inverting the hash function.
Though brute-force attacks (e.g. dictionary attacks) may be used to try to invert a hash function, they can become infeasible when the set of possible passwords is large enough. An alternative to brute-force is to use precomputed hash chain tables. Rainbow tables are a special kind of such table that overcome certain technical difficulties. Wikipedia

The Passwords Most Used By CEOs Are Startlingly Dumb (pcgamer.com) 94

Posted by BeauHD on Wednesday May 18, 2022 @07:20PM from the failing-to-set-a-good-example dept.
A recent cybersecurity report shows how immensely idiotic many CEOs and business owners can be, considering the strength of their chosen account passwords. PC Gamer reports: The research comes from NordPass password manager which identified back in 2020 that the general public's most commonly used passwords were sequential numbers like '123456', 'picture1', and yep, you guessed it: 'password'. The more recent research sample consists of 290 million cybersecurity data breaches around the globe, and denotes the job level of those affected. Turns out, when it comes to CEOs and other high-ranking businesses execs, their password choices are much the same as the general public, although many often feature names. Tiffany was spotted in 100,534 breaches; then there was Charlie with 33,699; Michael was found 10,647 times; and Jordan, 10,472 times.
The report also ranks mythical creatures and animals as some of the top passwords to have been cracked in data breaches. 'Dragon' was spotted 11,926 times, and 'monkey' comes in at 11,675. I spoke to IT support engineer Ash Smith, who recommends that companies should consider handing out randomly generated passwords as new accounts are created. "Arguably the strongest passwords are 3 random words, something that you can make a story about in your head to help you remember," he says.

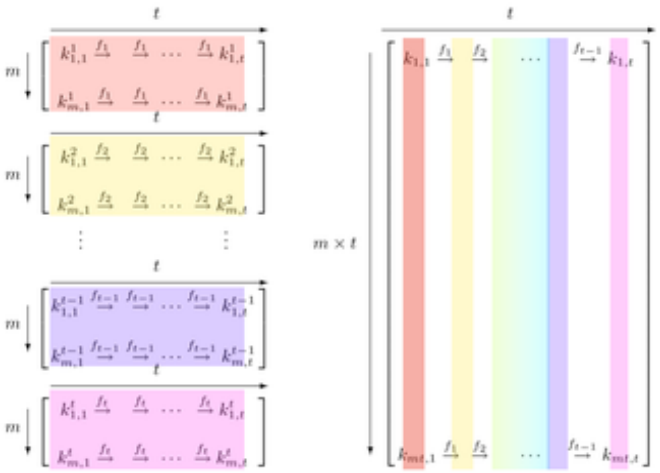
https://www.pcgamer.com/the-passwords-most-used-by-ceos-are-startlingly-dumb/

Subjected to brute force attacks

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search. Wikipedia

Rainbow tables

A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space–time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. Use of a key derivation that employs a salt makes this attack infeasible. Wikipedia



Rainbow table

In an email conversation with Micah Lee of EFF:

On 4/15/19 11:01 AM, n0stis wrote:

Right, but I don't know what made them think they could recover the password from the hash. I have never heard of this being done. Although this was Mendax, the guy who reportedly could move satellites over a dial up connection. :-)

"Experts" like Malcolm Nance are saying on MSNBC that Assange got Manning the network password to do the downloading. I guess he didn't bother to read the indictment like you did.

Interesting that analysts like Manning apparently had wide network privileges, could write cd's, but no local machine admin. I think I would have blanked all the passwords and blamed it on Windows, or found a way to DoD wipe the whole machine.

-----Original Message-----

From: Micah Lee [mailto:micah.lee@theintercept.com]

Sent: Monday, April 15, 2019 1:17 PM

Subject: Re: Assange

It's totally possible to recover passwords from hashes, but only if the passwords are weak. This is what "password cracking" normally means -- hashing a huge list of potential passwords (even so far as "all alphanumeric strings less than 8 characters"), and each time checking to see if the hash you end up with matches the one you're trying to crack.

If you look at the last 5 paragraphs of this 2011 article that was covering Manning's trial at the time:

https://www.politico.com/story/2011/12/defense-manning-was-overcharged-070787?paginate=false

It describes the exact stuff in the indictment, and says: 'The user alleged to be Assange replied that he had access to "rainbow tables," a type of data set that can be used to convert an encrypted password into plain text.'

A rainbow table is a pre-computed database that matches passwords to their hashes. So if a Windows user uses a weak password that's in a rainbow table, then their hash will be in it too, and someone with access to this rainbow table could quickly recover the password if all they have is the hash.

If you "salt" a hash, it makes it secure against rainbow tables. But also, there's a password cracking tool called hashcat that uses GPUs to crack passwords that are hashed with a wide variety of hash algorithms in real-time, without having to rely on rainbow tables (which is slower). Interesting stuff.

Micah Lee is First Look Media's Director of Information Security. He is a computer security engineer and an open-source software developer who writes about technical topics like digital and operational security, encryption tools, whistleblowing, and hacking using language that everyone can understand without dumbing it down. He develops security and privacy tools such as OnionShare, Dangerzone, and semiphemeral.
Before joining The Intercept, he worked as a staff technologist at the Electronic Frontier Foundation, where he explained how technologies work to journalists and lawyers, and worked to encrypt the web. He is a founder and board member of the Freedom of the Press Foundation, a member of the Distributed Denial of Secrets advisory board, and a Tor Project core contributor.
Send encrypted text messages to Micah Lee to +1-202-860-3151 on Signal or @micahflee on Keybase.

Note: Keybase is a key directory that maps social media identities to encryption keys in a publicly auditable manner. Additionally it offers an end-to-end encrypted chat and cloud storage system, called Keybase Chat and the Keybase Filesystem respectively. Wikipedia

Solutions

Random password generation

A random password generator is software program or hardware device that takes input from a random or pseudo-random number generator and automatically generates a password. Random passwords can be generated manually, using simple sources of randomness such as dice or coins, or they can be generated using a computer.

While there are many examples of "random" password generator programs available on the Internet, generating randomness can be tricky and many programs do not generate random characters in a way that ensures strong

security. A common recommendation is to use open source security tools where possible since they allow independent checks on the quality of the methods used. Note that simply generating a password at random does not ensure the password is a strong password, because it is possible, although highly unlikely, to generate an easily guessed or cracked password. In fact, there is no need at all for a password to have been produced by a perfectly random process: it just needs to be sufficiently difficult to guess.
A password generator can be part of a password manager. When a password policy enforces complex rules, it can be easier to use a password generator based on that set of rules than to manually create passwords. Wikipedia

An example: https://www.expressvpn.com/password-generator (there is an offline downloadable version of this)

If you are an American citizen or American business and the President of the United States asks for the support of these citizens and corporations to tighten up their digital security to protect against cyber-attacks by our numerous foreign adversaries by implementing 2FA and they mostly refuse.

They are: (select one)

1. Patriots (citizens)
2. Collaborators (insurrectionists)
3. Traitors (propagandists)
4. Stupid (uninformed)
5. Greedy (coin-operated)

Online banking primer: Use virtual keypad for safe transaction

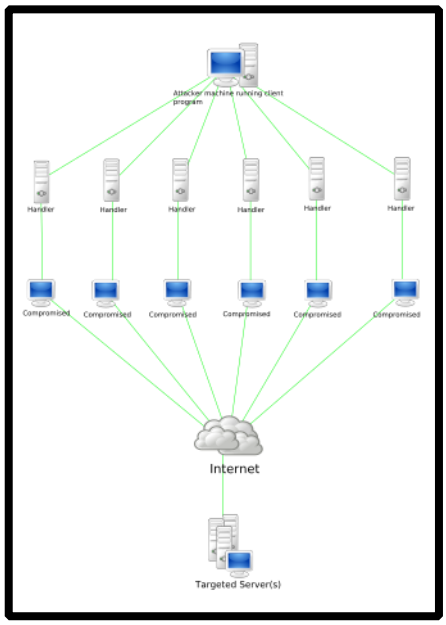
Synopsis

Virtual keypad is an online application, which substitutes the actual physical keyboard with a mouse.

It is easy for fraudsters to hack your internet banking password by capturing your keystrokes on your keyboard. This is possible through couple of programmes called 'Spy Ware' and 'Trojan Programmes', which are primarily designed to capture these strokes.

Read more at:
https://economictimes.indiatimes.com/industry/banking/finance/banking/online-banking-primer-use-virtual-keypad-for-safe-transaction/articleshow/7512038.cms

DDoS



Distributed Denial of Service or DDoS attacks are executed against websites and networks of selected victims. DDoS attacks happen on the Clear Web and the Dark Web but they are better protected against on the DW and thus less common.

https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack

Distributed Denial-of-Service as a Service

Some vendors provide so-called "booter" or "stresser" services, which have simple web-based front ends, and accept payment over the web. Marketed and promoted as stress-testing tools, they can be used to perform unauthorized denial-of-service attacks, and allow technically unsophisticated attackers access to sophisticated attack tools. Usually powered by a botnet, the traffic produced by a consumer stresser can range anywhere from 5-50 Gbit/s, which can deny the average home user Internet access.

Attack tools

In cases such as MyDoom and Slowloris the tools are embedded in malware and launch their attacks without the knowledge of the system owner. Stacheldraht is a classic example of a DDoS tool. It uses a layered structure where the attacker uses a client program to connect to handlers which are compromised systems that issue commands to the zombie agents which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker using automated routines to exploit vulnerabilities in programs that accept up to a thousand agents with remote connections running on the targeted remote hosts.

In other cases a machine may become part of a DDoS attack with the owner's consent, for example, in Operation Payback organized by the group Anonymous. The Low Orbit Ion Cannon has typically been used in this way. Along with High Orbit Ion Cannon a wide variety of DDoS tools are available today, including paid and free versions, with different features available. There is an underground market for these in hacker-related forums and IRC channels.

These attacks on the Internet are not to be confused with Distributed Denial of Secrets:

> Abbreviated DDoSecrets, is a non-profit whistleblower site for news leaks founded in 2018. Sometimes referred to as a successor to WikiLeaks, it is best known for its June 2020 publication of a large collection of internal police documents, known as Blue Leaks. The group has also published data on Russian oligarchs, fascist groups, shell companies, tax havens and banking in the Caymans, as well as hosting data scraped from Parler in January 2021 and from the February 2021 Gab leak.

https://en.wikipedia.org/wiki/Distributed_Denial_of_Secrets

SIM swap scam

> A SIM swap scam (also known as port-out scam, SIM splitting, Smishing and simjacking, SIM swapping) is a type of account takeover fraud that generally targets a weakness in two-factor authentication and two-step verification in which the second factor or step is a text message (SMS) or call placed to a mobile telephone.

https://en.wikipedia.org/wiki/SIM_swap_scam

It's one thing for tech companies to urge users to enable multi- **or two-factor authentication**, but now the **White House** is urging **all US organizations** to do it because of potential cyberattacks ahead.

Two-factor or multi-factor authentication (MFA) was a concept that needed to be explained carefully to the public a few years ago. It's an approach to cybersecurity that requires users to sign in to an account with something they physically possess, such as a phone.

Most companies don't use it, even when it's readily available, according to previously reported data from Microsoft, **because they prioritize easy access to information over security.**

https://www.zdnet.com/article/white-house-warns-do-these-8-things-now-to-boost-your-security-ahead-of-potential-russian-cyberattacks/

SIM hijacking:

2FA is a seemingly strong security standard, but if you are unlucky enough to become a victim of SIM hijacking, this layer of security means very little. SIM-swapping occurs when a cybercriminal poses as you to a service provider, such as AT&T, using social engineering techniques and information gathered about you to fool employees into transferring ownership of your mobile number.

Once they have secured your phone number, they have a small window of time to hijack online accounts -- such as emails, bank accounts, or cryptocurrency wallets -- before you notice your service has ended. In this time, attackers may be able to access 2FA codes.

AT&T has become the subject of multiple lawsuits centered around customers who allegedly lost millions in cryptocurrency due to SIM-swap attacks.

This type of fraud is difficult to protect against. However, one way to do so is to connect 2FA telephone numbers to a secondary number that is not publicly known and so could only become subject to a SIM-swap if leaked elsewhere.

https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/

GitHub Will Require All Code Contributors To Use 2FA (theverge.com) 84

Posted by BeauHD on Wednesday May 04, 2022 @06:40PM from the time-to-cough-up-your-phone-number dept.

GitHub, the code hosting platform used by tens of millions of software developers around the world, announced today that all users who upload code to the site will need to enable one or more forms of two-factor authentication (2FA) by the end of 2023 in order to continue using the platform. The Verge reports: The new policy was announced Wednesday in a blog post by GitHub's chief security officer (CSO) Mike Hanley, which highlighted the Microsoft-owned platform's role in protecting the integrity of the software development process in the face of threats created by bad actors taking over developers' accounts. "The software supply chain starts with the developer," Hanley wrote. "Developer accounts are frequent targets for social engineering and account takeover, and protecting developers from these types of attacks is the first and most critical step toward securing the supply chain."

Even though multi-factor authentication provides significant additional protection to online accounts, GitHub's internal research shows that only around 16.5 percent of active users (roughly one in six) currently enable the enhanced security measures on their accounts -- a surprisingly low figure

given that the platform's user base should be aware of the risks of password-only protection. By steering these users towards a higher minimum standard of account protection, GitHub hopes to boost the overall security of the software development community as a whole, Hanley told The Verge. "GitHub is in a unique position here, just by virtue of the vast majority of open source and creator communities living on GitHub.com, that we can have a significant positive impact on the security of the overall ecosystem by raising the bar from a security hygiene perspective," Hanley said. "We feel like it's really one of the best ecosystem-wide benefits that we can provide, and we're committed to making sure that we work through any of the challenges or obstacles to making sure that there's successful adoption."

Some top 100,000 websites collect everything you type—before you hit submit

A number of websites include keyloggers that covertly snag your keyboard inputs.

Lily Hay Newman, wired.com - 5/14/2022, 6:00 AM

When you sign up for a newsletter, make a hotel reservation, or check out online, you probably take for granted that if you mistype your email address three times or change your mind and X out of the page, it doesn't matter. Nothing actually happens until you hit the Submit button, right? Well, maybe not. As with so many assumptions about the web, this isn't always the case, according to new research: A surprising number of websites are collecting some or all of your data as you type it into a digital form.

Senate Report Finds Government is Unprepared To Stop Ransomware Attacks (fastcompany.com) 12

Posted by msmash on Thursday May 26, 2022 @10:49AM from the closer-look dept.

In the past few years, ransomware attacks have crippled schools, hospitals, city governments, and pipelines. Yet, despite the heavy toll such incidents have on both the public and private sectors, government officials have only a limited understanding of ransomware attacks and how cryptocurrencies are being used to collect payment, according to a new report from the Senate Homeland Security and Governmental Affairs Committee. From a report: "Cryptocurrencies -- which allow criminals to quickly extort huge sums of money, can be anonymized, and do not have consistently enforced compliance with regulations, especially for foreign-based attackers -- have further enabled cybercriminals to commit disruptive ransomware attacks that threaten our national and economic security," said Michigan Senator Gary Peters, the committee's chair, in a statement. "My report shows that the federal government lacks the necessary information to deter and prevent these attacks, and to hold foreign adversaries and cybercriminals accountable for perpetrating them."

Part of the issue is in reporting: The federal government doesn't have a standardized place for victims to log ransomware attacks, which typically

encrypt data until a ransom is paid in cryptocurrency. Both the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have websites where victims can report incidents, and some people report the attacks directly to their local FBI field offices -- all of which can leave people unsure of where to turn and lead to different agencies having records of different incidents. Financial regulators, including the Treasury Department's Financial Crimes Enforcement Network, also gather some data on ransomware, particularly around payments, but it's also far from comprehensive. A new law passed by Congress in March, as part of a broad government funding bill, will soon require operators of "critical infrastructure" to report to CISA within 72 hours when they've been the victims of a "substantial cyber incident," and within 24 hours of paying a ransom, but the provision hasn't yet gone into effect, pending regulatory decisions by CISA.

Companies are Subtly Tricking Users Online with 'Dark Patterns' (cnn.com) 41

Posted by EditorDavid on Saturday July 16, 2022 @05:34PM from the quiet-coercion dept.

CNN reports: An "unsubscribe" option that's a little too hard to find. A tiny box you click, thinking it simply takes you to the next page, but it also grants access to your data. And any number of unexpected charges that appear during checkout that weren't made clearer earlier in the process. Countless popular websites and apps, from retailers and travel services to social media companies, make use of so-called "dark patterns," or gently coercive design tactics that critics say are used to manipulate peoples' digital behaviors.

The term "dark patterns" was coined by Harry Brignull, a U.K.-based user experience specialist and researcher of human-computer interactions. Brignull began noticing that when he reported to one of his clients that most test subjects felt deceived by an aspect of their website or app design, the client seemed to welcome the feedback. "That was always intriguing for me as a researcher, because normally the name of the game is to find the flaws and fix them," Brignull told CNN Business. "Now we're finding 'flaws' that the client seems to like, and want to keep."

To put it in the parlance of Silicon Valley, he realized it was a feature, not a bug....

Brignull, for his part, said he has spent time testifying as an expert witness in some class action lawsuits related to dark patterns in the UK. "The scams don't work when the victim knows what the scammer is trying to do," Brignull said. "If they know what the scam is, then they're not going to get taken in — and that's why I've enjoyed so much exposing these things, and showing it to other consumers." The article notes that America's Federal Trade Commission "is ramping up its enforcement in response to 'a rising number of complaints about the financial harms caused by deceptive sign-up tactics, including unauthorized charges or ongoing billing that is impossible cancel.'"

Navigating the Dark Web

Or the

DARK SIDE OF CYBERSPACE

When was the Dark Web invented?

The term "Dark Web" was officially coined on 20th March 2000. It came with the introduction of the Freenet decentralized network system invented by Ian Clarke[35]. The intention was to offer access to a network that was more difficult for official sources to spy or intrude on.

To be anonymous on the Dark Web you need an anonymizer like TOR, The Onion Router, which is a web browser, and the only way you can view the onion sites. But even then, your ISP, Internet Service Provider may see your location address and will sometimes block (i.e. Comcast) users of TOR, as they fear that you might be engaged in illegal behavior. So you will need to be anonymous to them as well by using a VPN or Virtual Private Network and connecting to it first before starting Tor.

You can think of it this way, if you send a message or request a website address across the Internet, anyone who processes it can see your location, content, and destination of your clear text. If you encrypt your content and spoof your location (TOR), only your ISP can see your source and destination address. However, since the final leg from the Tor exit node is clear text, a VPN will encrypt all the way to the destination site.

If you use a VPN, your ISP cannot see your traffic, just that you are using a VPN. Your VPN provider can see you however, so choose carefully.

[35] *Ian Clarke is the original designer and lead developer of Freenet.*

Just How Deep is the Deep Web?

According to data from Wikipedia in the year 2000, Clear Web had a size of 167 Terabytes, while the Deep Web had a size of 7,500 Terabytes, which means that the content of the Deep Web (which contains the Dark Web) was 45 times greater than the information to which we have direct access. Currently, the University of California at Berkeley estimates that the actual size of the deep network is 91,000 Terabytes.

Note: you should use a VPN that does not create log files, which could be legally subpoenaed. A free VPN might be collecting data from you, so choose your provider carefully.

Note: The NSA can store encrypted data, waiting for later, many years perhaps, for processing with more powerful quantum computers.

Things you should know:

- Who owns the Tor exit nodes and are they logging all the traffic through it?
- If your computer is infected, or the cyber café being used (not recommended) is, you are screwed.
- If any servers you connect to are compromised, you are screwed.

Are there bad things on the Dark Web?

According to Peter Yeung, a writer for Motherboard, the Dark Web offers idealism, lightheartedness, and community as well as the illegal, immoral, and grotesque.

Besides selling personal data and compromised accounts, cybercriminals also trade and sell the elements for needed to launch cyber-attacks, espionage, and other malicious activities on the Dark Web:

Off-the-shelf software exploits (exploit kits) – toolkits that cybercriminals use to attack vulnerabilities in systems so they can then distribute malware.

Ready-to-use mal-icious soft-ware (malware) – ransomware, information stealers, Keyloggers (to record every key pressed on a device), spyware, adware, rootkits (notoriously difficult to spot and stop), Trojans and worms (with self-replicating capabilities).

Malware-as-a-service – a subscription-based model that rents the software and hardware cybercriminals need to carry out attacks, complete with malicious software, a distribution network, a range of targets and even technical support, and a personal dashboard to manage the project.

Software vulnerabilities - unknown to the software maker (called zero-days). Cybercriminals can use this to infiltrate organizations without being easily spotted.

Access to networks of compromised devices (botnets) - supply the computing resources hackers need to carry out their attacks.

Distributed denial of service (DDoS) - offerings which pool the power of extensive botnets to flood victims' systems with so much traffic that it takes them offline along with the services they supply.

Cybercriminal training - via tutorials, guides, and other types of content that support the upskilling of bad actors in various roles.

Money laundering (money mulling) - enables scammers to move around the money that they steal, extort, or otherwise take from their victims — and turn it into clean, untraceable cash.

https://www.aura.com/learn/dark-web

There Are 24.6 Billion Pairs of Credentials For Sale On Dark Web (theregister.com) 44

More than half of the 24.6 billion stolen credential pairs available for sale on the dark web were exposed in the past year, the Digital Shadows Research Team has found. Data recorded from last year reflected a 64 percent increase over 2020's total which is a significant slowdown compared to the two years preceding 2020. Between 2018 and 2020, the number of credentials for sale shot up by 300 percent, the report said. Of the 24.6 billion credentials for sale, 6.7 billion of the pairs are unique, an increase of 1.7 billion over two years.

With all those credentials available for sale online, account takeover attacks have proliferated as well, the report said. Seventy-five percent of the passwords for sale online were not unique, noted Digital Shadows, which said everyone needs to be wary. Proactive account protection, consistent application of good authentication habits, and awareness of one's organizational digital footprint are necessary to protect against account takeover attacks. Individuals, the report said, should "use multi-factor authentication, password managers, and complex, unique passwords."

What is Keystroke Logging and what are Keyloggers?

Keyloggers are built for the act of keystroke logging — creating records of everything you type on a computer or mobile keyboard. These are used to quietly monitor your computer activity while you use your devices as normal. Keyloggers are used for legitimate purposes like feedback for software development but can be misused by criminals to steal your data.

https://www.kaspersky.com/resource-center/definitions/keylogger

https://en.wikipedia.org/wiki/Keystroke_logging

Anti-keylogger

An anti-keylogger (or anti–keystroke logger) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on a computer. In comparison to most anti-virus or anti-spyware software, the primary difference is that an anti-keylogger does not make a distinction between a legitimate keystroke-logging program and an illegitimate keystroke-logging program (such as malware); all keystroke-logging programs are flagged and optionally removed, whether they appear to be legitimate keystroke-logging software or not. The anti-keylogger is efficient in managing malicious users. It can detect the keyloggers and terminate them from the system.

https://en.wikipedia.org/wiki/Anti-keylogger

The free version of SpyShelter runs in the background as a tray icon in Windows.

https://www.spyshelter.com/

Botnet Definition

Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term “botnet” is formed from the word’s “robot” and “network.” Assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution.

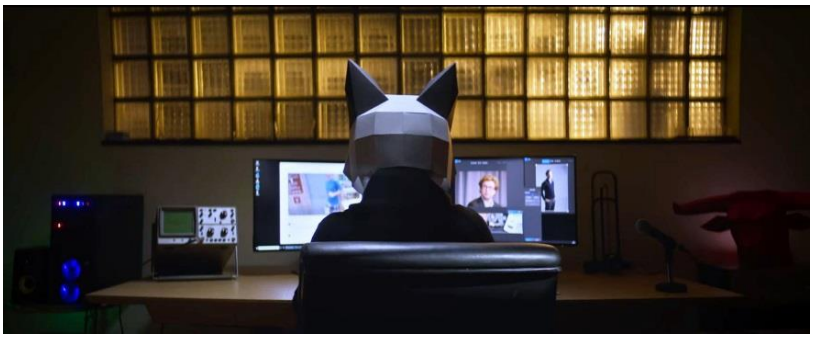
https://www.kaspersky.com/resource-center/threats/botnet-attacks

https://en.wikipedia.org/wiki/Botnet

Tales from the Dark Web

http://www.the_insider_goes_deep/tales1.html

Part One: Who am I and why am I here?



Most all of the main stream media paint the Dark Web as a shadowy digital underworld awash with nefarious characters who spend their time pedaling drugs, sharing illicit images, and recruiting for terrorist organizations. This may be true to an extent, but there is far more to the Deep Web than pedophiles seeking their prey, and criminals trading firearms for bitcoin.

Some report that 80% of traffic on the Dark Web relates to pedophile activity. Logic and my experiences to this point make me doubtful of this.

Wishing to be free from the constant surveillance of the regular net its users seek to have a secure concealed presence online.

You will find things there such as Underground Book Clubs, home to many banned books.

You may find Digital Advertising, where companies seek to attract the more technologically savvy and forward-thinking types, with innovative and cutting-edge advertising techniques.

There will be of course Anonymous Cat Facts with cat memes proliferating across any and every corner of the Internet like a digital epidemic.

A place for announcing New Music, by little known artists.

Speaking of epidemics there is of course Social Media, and in particular, Facebook but you should not trust it any more that you do on the Clear Web.

There are those seeking to evade Cyber-stalkers, as victims of cyberstalking can find some refuge in the Deep Web and can seek help anonymously and out of danger.

There are those who are editing and creating content for Wikipedia, which is dangerous in many foreign countries.

Some are political dissidents whose presence on the Dark Web is essential for resisting online censorship and state repression.

There are digital vigilantes who expose child abusers by hunting down those who live in this dark world.

There are many journalists and whistleblowers whose freedom of speech reporting on corruption in governments and businesses put them in jeopardy ala Julian Assange.

Law enforcement is maintaining a presence on the DW to monitor criminal behavior and bust some punks. Law enforcement credits the software for the exposure and prosecution of human trafficking rings in the U.S. and abroad, according to Scientific American.

Intelligence agencies continue to look for terrorists, or those that they can make people believe are terrorists.

Cybersecurity experts monitor exchanges where sophisticated adversaries often engage in discussions about hacking topics. By eavesdropping on these conversations, security analysts can gain insight into new and emerging threats.

Leveraging previously unindexed data on the Dark Web also helps fight money laundering by correlating bitcoin addresses with illegal activities. Security analysts can locate the places where illegal trade is happening as a means of luring the criminals into a trap.

For corporations and governments, the Dark Web is a relatively safe place to keep and limit access to sensitive information, whether company records or political intelligence. Law enforcement uses the Dark Web to hide its identity while visiting websites and to create fake sites to bait wrongdoers.

So this is what his research told him, secondhand or more distant from the original source. n0stis however thought that he really needed to go directly to the horse's mouth so to speak, and get his info directly from the DW'ers.

Sample message.

/u/n0stis in /D/Dread

Message the Mods

Hi all,

Just got to the DW and here. I am primarily interested in doing research on ISP DW hosting/colocation, and also having ongoing conversations on DW related topics like how and why people are using this section of cyberspace.

I want to find the best and most active Forums to do this.

Thanks for any and all assistance. n0stis

A new message thread

is dread one of the biggest forums on the dw or are there others like that?

by /u/altf4forever in /d/Dread

Quote: is dread one of the biggest forums on the dw or are there others like that?

14 comments

/u/capobianco

Response: Even my grandparents know about dread, so definitely

/u/mouquet_farm

Response: based granny selling her oxy scripts on the dw

/u/partygirlinc

Response: This is the humor I come here for ;)

/u/updatus

Response: hahahaha

/u/CarlosMartinez

Response: damn really? lol

/u/browndog

Response: Yes, a lot. we don't have to lie here. there are forums like: The Hub, Majestic Garden, Breaking Bad which are pretty good and big as well.

/u/brsSoftware

Response: i guess nulled or 4chan have more big community than dread. but i cant find 4chan or nulled on the dw

/u/updatus

Response: the fact that 4chan uses java, blocks Tor posting, and blocks VPNs is a huge red flag

/u/picassowhy

Response: NOTHING COMPARES TO DREAD FOR SHARING INFORMATION AND NETWORKING ON THE DNMs. Shout out to the mods and creators!

/u/ruinitall

Response: ***I'm not sure if it's the biggest but I do know thats it's more active than others I have seen. And for the most part we are all here for a common goal. The specific may vary from user to user but we are all looking to have a place where we can be free from the traditional rules and regulations of society.***

/u/GH05T187

Quote: "to have a place where we can be free from the traditional rules and regulations of society." this is a fact.

/u/SHERIFF

/u/AutoModerator M Judge Dread

We don't allow unknown onion URLs to be posted without approval. Please contact us via Mod Mail with a link to your post if you feel this was in error.

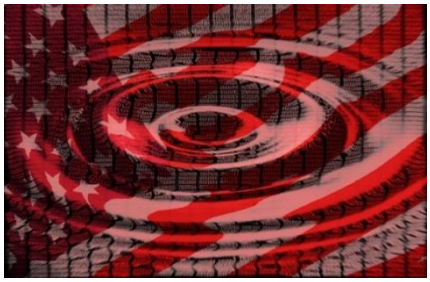
This comment was posted automatically by a bot. All AutoModerator settings are configured by individual communities. Contact this community's Moderators to have your post approved if you believe this was in error.

/u/JimmyHopkins

Response: Dread seems pretty active for a dw forum. It's nice.

The specifics may vary from user to user but we are all looking to have a place where we can be free from the traditional rules and regulations of society.

Or do not follow the rules.



https://www.mr-stingy.com/societys-rules-good-if-dont-think/

In each case, civil resistance by ordinary members of the public trumped the political elite to achieve radical change.

There are, of course, many ethical reasons to use nonviolent strategies. But compelling research by Erica Chenoweth, a political scientist at Harvard University, confirms that civil disobedience is not only the moral choice; it is also the most powerful way of shaping world politics – by a long way.

> Looking at hundreds of campaigns over the last century, Chenoweth found that nonviolent campaigns are twice as likely to achieve their goals as violent campaigns. And although the exact dynamics will depend on many factors, she has shown it takes around **3.5%** of the population actively participating in the protests to ensure serious political change.
>
> *https://www.bbc.com/future/article/20190513-it-only-takes-35-of-people-to-change-the-world*

> "Here's to the crazy ones. The misfits. The rebels. The troublemakers. **The round pegs in the square holes**. The ones who see things differently. They're not fond of rules. And they have no respect for the status quo. You can quote them, disagree with them, glorify or vilify them. About the only thing you can't do is ignore them. Because they change things. They push the human race forward. And while some may see them as the crazy ones, we see genius. Because the people who are crazy enough to think they can change the world, are the ones who do."
>
> *— Rob Siltanen (Siltanen & Partners an advertising agency, located in El Segundo, California founded by Rob Siltanen)*

Actually, this is the correct idiom below, and it certainly makes more logical sense.

> "Square peg in a round hole" is an idiomatic expression which describes the unusual individualist who could not fit into a niche of their society. The metaphor was originated by Sydney Smith in "On the Conduct of the Understanding", one of a series of lectures on moral philosophy that he delivered at the Royal Institution in 1804–06. Wikipedia

Another DarkWeb sample:

n0stis on the Raddle Forum

Question: Where am I and why am I here?

The Dark Web provides:

Freedom of or from politics?

Less moderated discussions of world, national, or life events

Freedom of or from Internet advertising

Freedom from or of Internet surveillance

Freedom of or from religion

Fool wrote

Reply to Where am I and why am I here? by n0stis

> *Where am I and why am I here?*

You are in the void, because you are in the void.

Veuzi wrote

Reply to Where am I and why am I here? by n0stis

This is an anarchist alt-reddit on the clearnet (raddle.me) with a darknet option. There's not that much more to it.

zoom_zip wrote

Reply to Where am I and why am I here? by n0stis

if it's too dark, you can turn on light theme in settings

SnowCode wrote

Reply to Where am I and why am I here? by n0stis

I think you're lost ahah. This site only has an option to use Tor, but it's also available on any normal web browser (on raddle.me).

The dark web doesn't provide you anything except having access to Tor-only websites (and therefore anonymize your internet traffic to those sites)

ziq wrote

Reply to Where am I and why am I here? by n0stis

this isn't the darkweb

n0stis response:

Thanks for the info.

To be clear, you are saying that the onion site http://c32zjeghcp5tj3kb72pltz56piei66drc63vkhn5yixiyk4cmerrjtid.onion/ is just a mirror of raddle.me?

Yes, that is correct.

- *The Hub »*
- *General Discussion »*
- *Where am I and why am I here?*

Poll

The Dark Web provides:

You may only select up to 5 options.

- *Freedom of or from politics*
- *Less moderated discussions of world, national, or life events*
- *Freedom of or from Internet advertising*
- *Freedom from or of Internet surveillance*
- *Freedom of or from religion*

Author Topic: Where am I and why am I here? (Read 32 times)

n0stis

- *New Contributor*
- *Posts: 27*
- *Community Rating: +1/-0*

Where am I and why am I here?

I am a writer doing research for a historical novel about the Dark Web. I am not a journalist, but I am looking to have discussions with a number of people on a number of topics on dread, The Hub, Raddle and maybe Envoy.

I think that you as a Hub subscriber would be a good choice for me if you are willing. I am not looking to expose anything other than get some ideas of who and why people are here and what they are doing. Am interested in legal activities only.

I am looking to have discussions on these topics and others.

The Dark Web provides:

Freedom of or from politics?

Less moderated discussions of world, national, or life events

Freedom of or from Internet advertising

Freedom from or of Internet surveillance

Freedom of or from religion

Email n0stis@mail2tor.com

BenzoBore

- *Jr. Contributor*
- *Posts: 69*
- *Community Rating: +12/-0*
- *Фёдор Михайлович Достоевский translated from Russian: Fyodor Mikhailovich Dostoevsky,*

Re: Where am I and why am I here?

« Reply #1

- *Quote*

A writer that shows should not need to be told.

it is in the darkness that you discern the most light
"never liked chasing the dragon as I'd usually end up chasing my own tail" - Beni

Allegiance

- *Head Punch Monkey*
- *Global Moderator*
- *Legendary Contributor*
- *Posts: 3114*
- *Community Rating: +228/-77*
- *Drunk on power and high on Mod Crack*

Re: Where am I and why am I here?

« Reply #2

Quote: You are welcome to try, however you will probably find that seasoned DW veterans are very skiddish with these types of projects. Also, we are not opposed to your chosen topics but the reality is that political and religious discussions or debate is really not a thing here. Also you said nothing illegal, so you will find that effectively cuts your options. This is first and foremost a harm reduction forum that happens to have a bit of a sarcastic sense of humor, in which we discuss drugs, markets, OPSEC, etc.

I wish you good luck and ditch that Windows PC for your safety and security.

Allegiance

NEW SUB KEY AS OF 2022-02-16, PLEASE RE-IMPORT
"Allie often shares the mod crack with me " -T.P.V
"You don't have to be a weirdo to mod here but it helps " -Lucidity
"my wife is a non binary black transsexual amphibious all terrain attack trained doormat i beg your pardon very much
still smells fishy, you better wash behind your ears and other places too"- Benihana
"Anyone who doesn't like pineapple on pizza is a cunt" - Lucidity

n0stis

- *New Contributor*
- *Posts: 27*
- *Community Rating: +1/-0*

Re: Where am I and why am I here?

« Reply #3

Quote from: BenzoBore

A writer that shows should not need to be told.

n0stis: I have no idea what that means. Please explain.

- *New Contributor*

Re: Where am I and why am I here?

« Reply #4

Quote from: Allegiance

I wish you good luck and ditch that Windows PC for your safety and security.

allegiance

Response: With all due respect, you do not know how many machines I have, how they are equipped and what my level of OpSec actually is. I posted in a General Discussion Forum purposely and provided a Tor email for those too skittish to post here. Never assume you know who you are speaking with.

Am not looking for discussions or debates, just responses to some simple questions. How about you? Are you up for it?

Quote: Where am I and why am I here?

by /u/n0stis • 1 hour ago in /d/CafeDread

What does this statement mean to you?

"I want or need a place where we can be free from the traditional rules and regulations of society."

/u/capobianco

Quote: "I want or need a place where we can be free from the traditional rules and regulations of society."

Response: Typical 4channer mindset, off with their edginess, porn and a revolting hate towards certain people for no reason other than to be 'different'

/u/fohshizzle2 James Kwong YMCA

That you are a retarded teenager

/u/n0stis

You missed it by several hundred miles.

/u/fohshizzle2 James Kwong YMCA

Even worse

/u/n0stis

Listen to your mother, and respect your elders.

/u/IamLegion

post not going how you imagined it huh?

Response: /u/n0stis

Expected more intelligence from those who are smart enough to get here.

OTOH, you can just watch Oxford/Yale/Harvard educated politicians on TV think and speak like morons as well.

/u/n0stis

This has nothing to do with me posing a question, but instead the grade level of the responses.

I guess that the question I posed was what does that quote, I have taken from

someone elsewhere in a DW discussion, mean to you?

You seem to have opinions about people, labeling, castigating and all that, but can you actually form an opinion about a subject that relates to why you are here in dread? That is one measure of intelligence.

The only way my post would be pointless to you is if you don't actually know why you are here.

If you can't or don't want to answer fine. Maybe others will, or maybe not. But why spew raw sewage?

We both joined this site a month ago, so somehow I am a noob and you are not?

I would however rethink your immediate impulsive need to attack anything you don't at first blush like or don't understand.

It doesn't cost anyone anything to be kind.

BTW, you are several thousand miles off on your Q conspiracy theory. I am at least several decades older than you so be forewarned that I can certainly give as good as I get.

/u/IamLegion 1 points

you are a noob not because of when you registered but because you are a fish out of water. What do people stand to gain from answering this question that you asked? It is a pointless exercise and serves nothing but to help build a profile on a user. I've been lurking on the darkweb longer than I've been participating on Dread, so I understand that if I participate in a conversation it is because I stand to gain or contribute information to the DN community, or for the lulz which is also as valid a reason for opening my mouth. You on the other hand are trying to present yourself as intellectual but are actually coming off as a noob. So yeah, go back to Qanon where you belong

Qanon are a bunch of people who think they are plugged in to the loop but they are actually just a bunch of inbred morons who are too stupid to know they are stupid, worse yet, they actually think they are smart. Sound familiar to you? If youre not already a Qanon, you should really check them out you might find that you belong there

/u/n0stis

Wow, you really have a fixation with QAnon. Is your mother a member or something?

Quote: "What do people stand to gain from answering this question that you asked?"

An exchange of ideas, like any other conversation. Both sides may learn something in the process. It's called being a normal human I think.

Quote: " It is a pointless exercise and serves nothing but to help build a profile on a user. "

Paranoid much? You VPN in from god only knows where, you hop through

Tor entry, middle and exit servers located god only knows where, you mask your Mac address, use an OS that doesn't leak identifying info, and with all that anonymity you are fearful of expressing your thoughts and ideas because someone might learn who you are?

What is the point of the DW then? Just transactional to buy and sell drugs? Buy Valid-Fake Documents Online?

If LE can see your words, then they can certainly see your transactions.

/u/IamLegion 4 posts 127 comments

respect is earned, not given! I suggest you lurk more and understand how thinks work first before doing anything on this side of the internet. Peace!

/u/capobianco

Quote: "I want or need a place where we can be free from the traditional rules and regulations of society."

"Typical 4channer mindset, off with their edginess, porn and a revolting hate towards certain people for no reason other than to be 'different"

/u/n0stis

Please clarify your comment. I will assume that this barrage is not aimed at me, but that you are simply describing the mindset of someone who would say something like what I quoted. Am i correct?

/u/capobianco

Yes you are correct.

/u/n0stis

Thanks for the clarification.

Some harmless stupidity gets **a lot** of traction on The Hub.

- *The Hub » •Start Here » •For Beginners » •Pineapples on pizza Poll*

How do Y'all feel about pineapples on pizza

I refuse to try 308 (12.5%)

Nasty AF 471 (19.2%)

EH it's ok ig 427 (17.4%)

Pretty good 545 (22.2%)

That is my shit 707 (28.8%)

Total Members Voted: 1749

Pages: 1 ... 153 154 [155]

Author Topic: Pineapples on pizza ***(Read 357332 times)***

benihana

- *Moderator*
- *Jr. Contributor*
- *Posts: 73*

- *Community Rating: +430/-231*
- *reformed troll*

Re: Pineapples on pizza

« Reply #3080 on: March 02, 2022, 10:28:44 AM »

Quote from: legros on March 02, 2022, 12:17:03 AM

There are people who complain loudly about pineapple on pizza to be 'interesting'. They are not interesting. They just have bad taste.

you take that back, heathen

Thread by /u/HugBunter A in /d/OpSec

Response from: /u/newbieforever2018 "You've got ★bail★" 1 points

"And you make fun of me using Windows OS?"

/u/newbieforever2018

Dread message from (/u/n0stis):

-----BEGIN PGP MESSAGE-----

Version: BCPG v1.63

Tell me more?

Win7?

Thanks,

n0stis

-----END PGP MESSAGE-----

-----BEGIN PGP MESSAGE-----

/u/newbieforever2018

Quote: "If you look more closely it was a reply to the moderator of /d/opsec and my friend /u/headjanitor and meant as a joke. He knows that I don't use tails so I was just ribbing him because they found an exploit in Tails. Regardless Tails is far superior to Windows as a secure OS. I did not think that anyone would take me seriously. Have a good day!"

Response: Thanks for the response, which raises some questions.

So Tails requires a dedicated boot from an external image?

Tails requires an update before you can update Tor?

Tails isolates you from the rest of your computer OS applications and tools?

Tails requires a lot of time building new boot images?

Now can you give me some plusses versus a well-tuned Windows system?

Thanks,

n0stis

PS. whatever you are typing into puts two spaces after a period. This is not only typographically incorrect, ever since the single mono-spaced font

typewriter days, but is also a potential tell that you learned how to type on a typewriter. (This is of course the default behavior of some word processor software despite using proportional fonts)

/u/newbieforever2018

-----BEGIN PGP MESSAGE-----

Version: GnuPG v1

Quote: "I use windows, not tails. For the best info on tails please go to /d/tails"

Response: Did you mean Whonix or Qubes? You said you did not use Windows.

Quote: "Tails can be installed on a usb drive and leave no trace on the computer it is attached to or it can actually be installed as the main OS or a separate OS for a dual boot choice."

Response: Doesn't installing on a hard disk mostly defeat the purpose of it?

Quote: "If you are doing things that you want to stay hidden there are no well turned windows systems."

Response: Opinions without basis in fact are speculation at best, or superstition at worst and are contrary to computer science. Also, a bias against Microsoft as a company or Windows as an OS does not make for a valid basis for a discussion.

Care to enlighten a noob with the factual basis for your above statement?

n0stis

-----END PGP MESSAGE-----

-----BEGIN PGP MESSAGE-----

/u/n0stis

Quote: "I believe that you need to check your facts. Please screenshot or link me to where I said that I do not use windows. I DID say that I do not use Tails and you are best off going to /d/tails to find out info about it."

/u/newbieforever2018,

*Response: Ok, my bad. I had assumed by your tone: "**Regardless Tails is far superior to Windows as a secure OS. I did not think that anyone would take me seriously."** that you were mocking Windows and I wanted more detail. Such is the limitations of written communications.*

Quote: 1. Tails does not leak info the way that windows does so even if installed on your computer alongside windows it would be safer to use when doing dnm stuff compared to using windows.

Quote: 2. "If you are doing things that you want to stay hidden there are no well turned windows systems."

Quote: 3. Regardless Tails is far superior to Windows as a secure OS. I did

not think that anyone would take me seriously. If by well tuned you mean a windows system that runs at peak performance then we are talking about two different things. I am talking about opsec, not system performance. I do not need to justify my belief and if you disagree with that statement then I challenge you to go to /d/opsec and ask the experts if there is a way to make Windows OS as safe as Tails when doing things on the dnm. Then tag me in any reply that disagrees with my comment. I can barely believe that you are interrogating me when I have freely admitted that I know next to nothing about opsec ...

Response: Well I am not here to help educate you, although I might be willing answer Windows OpSec questions you might have. I was simply asking questions, to expand my experience on the DW and separate the facts from the bullshit. And also I was obviously talking about DW tuning and not system performance.

So you say that you know nothing about DW OpSec, but you still have expressed at least three fact-free opinions above.

What say you?

n0stis

-----END PGP MESSAGE-----

/u/newbieforever2018

-----BEGIN PGP MESSAGE----- The way that you are continuing this astounds me and yet did you do what I requested, find someone with good opsec knowledge to debunk my opnions and either screenshot their reply or link me to it? Nope

It is more like a religious zealot type thing offended you that I stated that it is highly unlikely that the Flying Spaghetti Monster actually exists despite numerous mentions of him available via internet search results. My opinons about FSM are fact free too.

I will clearly restate my "belief" that even though I use and love the windows os in no cases is it as safe when doing dnm related activities that one wants to remain private compared to doing the same activities using the Tails os.

You need not reply unless you can find some FACTS posted by someone with credentials in the opsec field who disagrees with my belief.

I also noted that you FAILED to point out where I stated that I do not use Windows. Funny how this just seems like an attack on me rather than an attempt to correct my beliefs.

-----END PGP MESSAGE-----

/u/n0stis

-----BEGIN PGP MESSAGE-----

Quote: "You need not reply unless you can find some FACTS posted by someone with credentials in the opsec field who disagrees with my belief.

I also noted that you FAILED to point out where I stated that I do not use Windows. Funny how this just seems like an attack on me rather than an attempt to correct my beliefs."

Response: I apologized for the original misunderstanding. I don't attack anything except ideas and speculation.

How do you know that I am not someone with those credentials?

I indicated that I was willing to help you, but I see now that you are not interested in learning.

So it appears as if we are both wasting our time.

n0stis

-----END PGP MESSAGE-----

-----BEGIN PGP MESSAGE-----

/u/newbieforever2018

I apologize. I had no idea that your purpose was to help me. I thought that you just wanted to argue with my assertion that tails is always safer than windows for doing dnm related things that one wants kept private. My wife kept corrupting the windows install on her computer to the point that I got sick of the ordeal of having to reinstall it so I popped an easy install Linux distro meant to replicate windows on there and now worst case I can have her back up in five minutes.

I just like my Windows and my friend on /d/opsec gave me some tips to change some settings to make my install safer than it was however I am not trying to learn. I am happy with my windows and the half dozen different web browsers that I run simultaneously on it with countless open tabs, all big no no.

It is definitely my idea, speculation, belief that Tails is safer in all cases but I have no link to "Bill Gates admits that he uses Tails instead of Windows on his personal machine".

Take care

-----END PGP MESSAGE-----

-----BEGIN PGP MESSAGE-----

Quote: "I apologize. I had no idea that your purpose was to help me. I thought that you just wanted to argue with my assertion that tails is always safer than windows for doing dnm related things that one wants kept private. "

Response: I picked this up on Envoy, views from two OpSec experts.

Rorschach_9000

Everyone who swears by Tails is definitely putting yourself at risk. It does nothing to protect your real IP address. Don't believe me, go ask William Gibson of Versus what os he uses & why.

Quote: "It is definitely my idea, speculation, belief that Tails is safer in all cases but I have no link to "Bill Gates admits that he uses Tails instead of Windows on his personal machine".

Response: I know you said this in jest, but I happened to run into this:

Bill Gates in PC Mag.

What's your everyday PC these days? How does it compare with the OG IBM PC?

I use a mix of devices depending on where I am and what I need. I have a cell phone with a big screen, the Samsung Galaxy Z Fold3. When I'm traveling, I use a Surface Laptop 4, one of Microsoft's products. And then on my home office desk, I have a Surface Studio 2 All-in-One PC.

I tend to use the big PC screen more than most people because I like sending long emails and reading long documents and research papers. I'm not quite as phone-centric as the younger generation, but the mix works well. I can stay on top of all my work at the foundation, even as I'm traveling. The tools just keep getting better, but there's still a long way to go and a lot of potential.

Now despite whatever bias you may or may not have against, paid commercial software, Microsoft, Windows or whatever, I will concede to you that about ten years ago there was a dramatic shift in Microsoft from being mostly benevolent to becoming mostly malevolent.

For you youngsters a bit of history. Microsoft and the clone PC builders are the reason that we have had this tremendous democratizing of the PC market that allowed most anyone to own a computer for the past 40 years. This would have never have happened with Unix or Apple or Xerox or IBM.

Despite all our human flaws, we continue to stand on the shoulders of giants like Vannevar Bush and Doug Engelbart (look them up) who imagined and advanced the idea of a machine that could serve as a memory device to augment and expand human thinking and problem solving.

That is all,

n0stis

-----END PGP MESSAGE-----

/u/newbieforever2018

"Of course I meant Windows compared to Tails. That does not mean that a vpn should not be added.

What OS does William Gibson use? I am guessing Whonix or Qubes or some linux variation but it would definitely shock me if he uses windows to run his market."

My point is that those who promote Tails as the "be all and end all", are as confused as those who say Windows is infinately bad because of telemetry.

See my exchanges with your buddy in OpSec.

n0stis

/u/newbieforever2018

Quote: Tails is easy to use out of the box for the average guy and has amnesia which windows NEVER does.

I am a benzo moderator, not IT. Sure Qubes and Whonix might be better than tails but also more complicated for average Joe

"Tails is easy to use out of the box for the average guy and has amnesia which windows NEVER does.

I am a benzo moderator, not IT. Sure Qubes and Whonix might be better than tails but also more complicated for average Joe"

Response: Rarely is security EASY. A false sense of security is however. As I indicated in /d/OpSec, all OS's require hardening.

n0stis

Privacy & Security Guides

http://elfqv3zjfegus3bgg5d7pv62eqght4h6sl6yjjhe7kjpi2s56bzgk2yd.onion/darkelf_tor_onion_tails_config.php

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/37ad1ab20b18bb2bbd6e

/u/newbieforever2018

Quote; "I never said that Tails is bullet proof, just that imho it is safer than windows and I am a windows user so I don't know what the endgame is here."

Response: I guess that I was looking for more than an opinion. I haven't seen any real proof of this opinion yet. I have seen bias's, speculation, and FUD, but not facts. Since you are not a CS guy, I think that we are done with this particular topic.

I will continue to bark up the /d/OpSec tree, but not having much luck there so far either.

It's like a legend that gets passed from one user to another until no one know the origin of the legend.

This will give you something to think about however.

https://www.theregister.com/2022/05/31/the_cynics_guide_to_linux/

n0stis

Insider Story One </html>

(the following is excerpted from The Cozening, Insider Story 1011)

Recent news reports told the story of the global data security collapse, Microsoft SpyGate, the forced update disaster, and the subsequent removal of Windows10 from the market having been discredited and purged as a data surveillance tool disguised as a computer operating system.

The President continued on to say that he had called with a personal invitation for them to visit the White House in the next week, and for each to receive the Presidential Medal of Freedom directly from him at a thank-you ceremony in the White House Rose Garden. He further explained that this award recognized those individuals who have made "an especially meritorious contribution to the security or national interests of the United States". "You have certainly earned this he exclaimed! You are also owed my sincerest personal apology for having been banished from the US, and a big "My Bad" for the whole mistaken Terrorist Watch and Do-Not-Fly List thing."

Following the medal ceremonies and parade, the Merry Band of Misfits and Malcontents testified before Congress on cyberspace security and encryption.

Most echoing and expanding on the thoughts of renowned security technologist Bruce Schneier.[36]

"We can all avoid and block surveillance with privacy enhancing technologies like web browser extensions. The most important of these techniques is of course encryption. Math will always defeat surveillance. End to end web encryption, hard disk encryption and email encryption are all now available to anyone. Be aware however, that metadata is not encrypted. So the contents of a letter are protected, but the contents of the envelope covering it are not. You can however leave the return address off the envelope, but using Tor will anonymize your location. Encryption will not protect your computer while in use, so it is not a total solution.

The US should adopt similar protections of personal data as the EU did with the Charter of Fundamental Rights.

Our point here is that politics can undermine technology, and that technology can undermine politics. Neither trumps the other. If we are going to fix things, we need to fight on both the technological and the political fronts."

---

[36] *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*

The group then also threatened to return their medals unless Snowden, Manning, and Assange were pardoned by end of the Obama Presidency in December of 2016. They also called for an immediate end to drone strikes in civilian areas everywhere in the world.

Not unlike his feelings on gay marriage, Obama had evolved and was evolving on mass surveillance in that having breakable or back doored encryption would just put everyone at risk.

Snowden did not release any information. He could have dumped the whole pile of shit on WikiLeaks and let Assange and his people sort it out like Manning did, but he did not. He was much more responsible, not to mention brave in the view of many.

He took a responsible path to allow journalists, New York Times, Washington Post, The Guardian, who do this on a daily basis, to decide what was released. This info went through the completely standard journalistic process, with multiple sources, review by the editors, publishers, etc.

Snowden knew enough that he could not trust his own bias's and was very thoughtful and smart about this. These journalists have the connections to government people who tell them what the down side of the release of information would be, thus bypassing the argument of putting people in harm's way. This is the Fourth Estate working as it should, and not being co-opted as it was during the lead up to the Iraq war.

Yet those in power, who literally had blood on their hands, projected that rebuke on Snowden and Assange.

I believe that Snowden fully understood the consequences of what he did and had thought this out for many years.

Daniel Ellsberg revealed the lies of Johnson and Nixon about the Vietnam War and is now considered a hero. This modern day equivalent is no different, civil disobedience (aka Good Trouble) at its finest.

I fully believe that Snowden will receive a Presidential pardon, not unlike the Vietnam War resisters did, and Oh how close n0stis was to being one of those.

End of excerpt.

What follows is the story of a group of humans, who perhaps looked to outsiders like a cross between Burning Man attendees and the hacker stereotype in popular media, which I (Lefty IRL, and n0stis or arister0s on the DW) recruited to create a team from the privacy and anonymity lovers from the Dark Web.

So we all set about building a new decentralized Web, Web 4.0. An Internet to serve the public, not the profiteers. We will of course, use the RealOS and its WinFS encrypted file system, as an entry client with a newly refreshed encrypted web browser and refreshed email client, as the building blocks for this new decentralized Web Mixnet.

Note: Returning readers of this Insider series of books will recall that in the Cozening (A Murder of Promise), the RealOS was given the ability to encrypt all files on a user's computer in storage, in transmission and most importantly while in use. How this fully homomorphic encryption or FHE, at the time 2014 the holy grail in the quest to keep data secure, was accomplished in the RealOS by our team was purposely kept as a closely guarded secret from the reader. This was done primarily for security purposes that were very relevant at that time during a global privacy breakdown, and the governments forced removal of Windows 10 from the market as explained in the earlier excerpt.

The new members of the team received a refresher course that explained that Fully Homomorphic[37] Encryption or FHE[38] provides data security that delivers mathematical proof of encryption by using cryptographic means to allow the performance of a computation by a computer. This prevents exposing data while in use to be potentially compromised by savvy adversaries or even accidental leaks.

FHE technology development at the time (2014) required a prohibitive amount of compute power and time. The RealOS team, with their technical advisors, developed a software stack to utilize unused cycles of the common multicore processors at the time providing the necessary acceleration. The performance penalty at the time for a computation that would take a millisecond to complete on a standard laptop would take weeks to compute on a conventional server running FHE. The engineering work that the RealOS team did reduced this processing time penalty from weeks to seconds, with calculations being performed in seconds per bit.

---

[37] Homomorphic encryption is a form of encryption with an additional evaluation capability for computing over encrypted data without access to the secret key. The result is that such a computation remains encrypted while being processed.

[38] FHE uses an algebraic system that allows working with data without requiring decryption first.

One goal with the RealOS update is to continue to lower the encrypted data computational speeds to the equivalent of what is seen in plaintext through the refinement of the algorithms. This will continue to enhance the user's ability to protect and preserve data as well as help ensure their privacy, while maintaining an acceptable level of performance.

The Web 4 group knew that the 4096-bit RSA standard had been broken via acoustic cryptanalysis, so they previously chose the 8192-bit code developed with co-inventor Leonard Adleman, and cryptography innovator Manuel Blum, to accomplish this critically important and massive task.

But now things continued to change and they looked for long-term security protection for thirty to fifty years (2022-2068), they knew that they needed to develop a 16384-bit Encryption Algorithm.

Back in 2014 that group used the Ed Roberts (MITS) missive that "software was just virtual hardware" to motivate the creation of the software stack to achieve the RealOS FHE. But now with the doubling of the encryption algorithm, they really would need an optional hardware accelerator.

This accelerator would be based on a Raspberry Pi and be available in PCI-Express bus versions for desktops and various USB configurations for laptops and tablets.

As previously mentioned, in the beginning there was the government funded ARPANET which begat the NFSNET which begat DARPANET, which begat the commercial Internet and then this privately funded Internet begat the open Web. Web 1.0 was a static web. Creator Tim Berners-Lee, scientists, professors, and later some businesses and individuals shared data mostly.

Then came Web 2.0- or the dynamic web which was created after the government turned over the public Internet to an oligopoly of corporate for profit interests for free. Over time and lack of regulation (self-regulation), it degenerated into something unrecognizable with unmoderated social media, endless and invasive advertising, corporate data harvesting, privacy theft, misinformation, and disinformation, all creating new dystopian realities.

Right now there are people are working on Web 3.0- with crypto currencies and a blockchain database with the goal of returning to an identity free, decentralized web. Except they are now using unsustainable and excessive resource intensive crypto mining and encountering disruptive market speculation. It is most likely to many, that venture (vulture) capitalists will replace the likes of Google and Facebook as the autocrats of Web 3.0 as this scenario plays out.

Vulture (oops I mean Venture) capitalists will likely end up ruling the Web 3.0 Internet world.

The original subsets of Web 2.0 were the Deep Web, for access controlled corporate and scientific data, and the Dark Web, not of much value beyond illegal drugs, porn, stolen passwords, fake documents, etc. and was a secure but *not* a suitable general replacement. The Dark Web requires excess CAPTCHA, as protection against invasive spam bots, and DDoS attacks by competing drug markets, and excessive and clunky encryption methods as protection against corporations, governments, hackers, and everyone else.

The only viable option we all as a group saw was to start anew under their beliefs that:

The Internet should operate as a single, decentralized network of networks – with global reach and governed through the multi-stakeholder approach, whereby governments and relevant authorities collaborate with academics, civil society, the private sector, technical community and others. Digital technologies reliant on the Internet will yield the greatest dividends when they operate as an open, free, global, interoperable, re-liable, and secure systems. Digital technologies should be produced, used, and governed in ways that enable trustworthy, free, and fair commerce; avoid unfair discrimination between, and ensure effective choice for, individual users; foster fair competition, encourage innovation and promote and protect human rights. Excerpted from: A Declaration for the Future of the Internet (April 2022)

As a group, they all believed that you should not have to worry about surveillance while online. Privacy should simply be the default of all of Cyberspace. The way the Internet operates today, the consequences of surveillance threaten all of us, from stolen funds and identities to profiling and human rights violations.

Cryptography or Crypto, is not only about cryptocurrency or coins, but has privacy-focused Cypherpunk roots. Without cryptography, individual privacy and certainly government or corporate whistleblowing are not possible.

This is because the existing internet protocols leak sensitive data (metadata) that can be de-anonymized and used without the user's knowledge.

The team then collaborated to develop a preliminary set of goals for this project:

- **First Goal: We will rebuild the RealOS's Internet Scout web browser to provide a built in VPN, not a simple browser extension (this VPN can be used traditionally to the requested endpoint, to a decentralized VPN (dVPN) or for entrance to the Tor network or to a Mixnet). We will rename the browser to Cyberspace Explorer to reflect its use for navigating Web 1 through Web 4 and the Dark Web.**

- **Second Goal: We will modify the Dark Mail email software to more fully integrate it into the RealOS, as well as upgrade the level and type of encryption, improve the PGP encryption/decryption engine to support html (rich text) fonts as well as graphics.**

- ***Third Goal: We will modify the RealOS WinFS file system to work on top of the Didgets operating system database to interoperate with the proposed P2P (Peer-to-Peer) Mixnet networks.***

- **Forth Goal: We will use a Mixnet, modeled after Nym[39], but public rather than private, to secure network level privacy. This network will protect even against the most powerful, adversaries that can observe every packet going in and out of your Internet connection. It will be engineered so that you can be online anytime and anywhere without the fear of being watched. This infrastructure will prevent any data leakage by protecting every packet's metadata at both the network and application layers.**

---

[39] The Nym network ("Nym") is a decentralized and incentivized infrastructure to provide privacy to a broad range of message-based applications and services. The core component of Nym is a Mixnet that protects network traffic metadata for applications, providing communication privacy superior to both VPNs and Tor against global adversaries that can watch the entire internet.

These product creations will be unlike anything accomplished before. There will be at least four very complex technologies developed here, not only make to work, but make to work in concert with each other for the benefit of the users and be invisible to them at the same time.[40]

Unlike the development of the original RealOS, (The Cozening) this group had *not* been banished from the US, put on the No-Fly and Terrorist Watch Lists, and forced to escape to Canada to do their work. That work had been done mostly as an assembled group, with some remote participants and during some mobile work and sightseeing travel.

Now with the worldwide pandemic looming, the need for anonymity, and a geographically disparate group, this work would be done almost exclusively via remote contact on individual emails, chats and group video conferencing.

All would be judged by their work product, not gender, ethnicity, or geographical location.

We fully believe that who you speak or write to, when you do, on what device, and how often should not be publically available information.

Jitsi video conferencing with the team

[40] *"Any sufficiently advanced technology is indistinguishable from magic." Sir Arthur Clarke's third law,*

- ***First Goal: We will rebuild the RealOS's Internet Scout web browser to provide a built in VPN, not a simple browser extension (this VPN can be used traditionally to the requested endpoint, to a decentralized VPN (dVPN) or for entrance to the Tor network or to a Mixnet). We will rename the browser to Cyberspace Explorer to reflect its use for navigating Web 1 through Web 4 and the Dark Web.***

For the first goal, we pulled together a team made up of /u/matter and /u/solar, and special advisors consisting of Tim Berners-Lee who will assist us with for the features of HTML5, and the best practices of the W3C[41] standards.

Using skeuomorphic design concepts, we will create a stable, speedy browser that can handle even the most multimedia-rich websites. It will support spatial navigation[42], where users will be able to traverse webpages by using only their keyboard.

/u/matter explains it this way, "in the past Web browsers have used tabbing navigation to change the focus within an interface, by pressing the tab key of a computer keyboard to focus on the next element (or ⇧ Shift+Tab ↹ to focus on the previous one). The order is based on that in the source document. For HTML without any style, this method usually works as the spatial location of the element is in the same order of the source document. However, with the introduction of style via presentational attributes or stylesheets such as CSS, this type of navigation is being used less often. Spatial navigation uses the arrow keys (with one or more modifier key held) to navigate on the "2D plane" of the interface. For example, pressing the "up" arrow key will focus on the closest focusable element on the top (relative to the current element). This can save many key presses."

/u/solar agreed and added that for users, "this allows a faster way to "jump" to different areas in long web pages or articles without manually scrolling and scanning with their eyes. Some examples include using the Tab ↹ key to jump to the next input field, but also the ⇧ Shift key with arrow keys (↑, ↓, →, ←) to jump to various links and text headers."

---

[41] World Wide Web Consortium w3.org. The World Wide Web Consortium is the main international standards organization for the World Wide Web. Founded in 1994 and currently led by Tim Berners-Lee, the consortium is made up of member organizations that maintain full-time staff working together in the development of standards for the World Wide Web. Wikipedia

[42] In computing, spatial navigation is the ability to navigate between focusable elements, such as hyperlinks and form controls, within a structured document or user interface according to the spatial location. This method is widely used in application software like web browsers and computer games.

Our group will be focused on an ad-free future, where monetization of data is not a goal, but reducing the amount of data that can be sold to target ads to people based on browsing behavior will be.

Also, getting away from Chromium engine browsers around will relieve people of the fear for their privacy and Google's exploitation of privacy concerns.

Bookmarks will have a new approach in Cyberspace Explorer (CE). Rather than having them stored in a drop-down that clumsily cascades vertically, bookmarks will be elegantly stored in a sidebar that is easy to manage and does not overwhelm the user.

The sidebar is more than just bookmarks though. It's also where you can manage your downloads, save your contacts and make notes. The group also plans to integrate the Dark Mail web client into the sidebar.

A visual-centric browser will have neat animations that give it a modern feel. It will discard traditional tabs in favor of new "visual tabs" where an icon of a site collects all the pages you have opened within the site. An algorithm intelligently pushes most-used tabs to a more prominent position on screen. It will also have a built-in gallery where you can drag-and-drop any image or video, or screenshot any part of the screen. You can then share these images or videos in another web page or chat with a similar drag-and-drop movement.

On the security side, the primary protocol all Web browsers currently use to encrypt their connections to websites, Transport Layer Security (TLS), can be attacked via traffic analysis to reveal the contents of encrypted communications. Analysis of network traffic metadata can also reveal the content of encrypted Domain Name. System (DNS) queries in protocols such as DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH).

Besides acting as a side channel that may reveal encrypted content the network-level metadata associated to online activities can be exploited to uniquely identify users, enable pervasive tracking, and reveal private information about personal or business activities. By applying "artificial intelligence" algorithms to metadata, it is possible to predict political preferences, associations, social relations, purchasing behavior and other intimate details of their private lives and minds. The current widespread corporate exploitation of metadata for advertising and sales purposes joins the evidence of metadata collection and analysis being carried out en masse by the US National Security Agency (NSA) and similar agencies around the world.

The Web 4 group's fourth goal of using a Mixnet will counteract this behavior.

The Web 4 group decides that during all of the hard work of creating a new web they will need some entertainment to let off some steam and sharpen their skills.

They will need to take an evil corporation down. Targets suggested include Google, Amazon, Facebook, Microsoft, and Apple.

To narrow it down, they decide that while evil, Microsoft and Apple at least have a few redeemable aspects.

Taking down Amazon would disrupt many people from getting their supplies, so they flip a coin. Tails its Facebook and heads its Facebook.

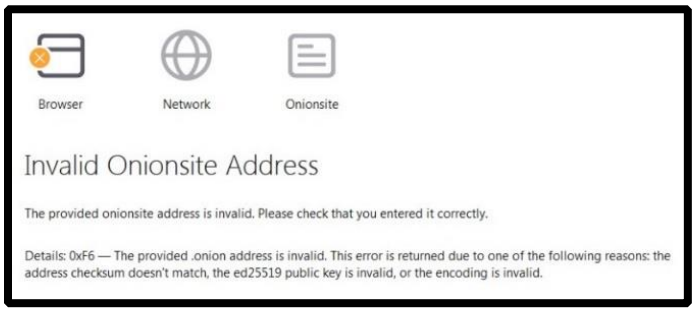
It comes up tails.

To be continued…

Part Two: You don’t have to go home, but you can't stay here.

http://www.the_insider_goes_deep/tales2.html

n0stis had not be able to connect to dread for several days, and then when he did finally connect he sees this message thread on the site.



DW website message when it is down

New Deployment Script, A Tighter Endgame, and Servers! Servers! Servers! Poll

by /u/Paris A /d/Dread

What an eventful few days! Hope you didn't miss us too much

A DDOS attacks just caused the dread guard nodes to cry bloody murder. I'm waiting for more servers to be accepted as guards into the tor network but until that moment happens we are running on a mirror system. Latency will be higher and it will be a bit unstable (with occasional 502s, but we will go back to the faster low latency cluster fronts once more guards are available for them.

All ads (and premium memberships) will be pushed back a few days. Think of it like a time skip where these past couple days didn't happen. If any ads did expire please let me know and I'll get it sorted out. As always no advertiser will pay for our downtime.

The i2p cluster will be getting a stability improvement in the coming days to make the tunnel connections, I hope, a little more stable.

We are not going anywhere.

/u/newbieforever2018 ☆Cares About Noobs☆

Thank you /u/paris

We were getting scared that the end days were here for dread, so great to be back

/u/TTTz P 2 year club Trophy

The Ultimate Exit - Enron Level - People Jumping From High Buildings - Chaos

It would be a perfect exit - After all the donations and purchases of mugs - mine is still in the mail - Shaky still not giving tracking

Being serious now, Just as Newbs said getting scared is not a good feeling. People all over had some random theories.

But overall I am glad I was able to get a small amount of sleep

Thanks Paris, the Whole Team and Paris for the slick update notice you posted somewhere as POL during the downtime

/u/LeChacal P

Thanks for the updates Paris. ASAP Market is also suffering DDOS and there is one motherfucking vendor who is said to his buyer that ASAP market, Dread, Recon, World are run by same team. We banned him.

[qutoe=Paris] We are not going anywhere. [/quote]

Same. ASAP Market is not going anywhere.

/u/Gladiator P

We know exactly who you mean!!!!!! Same with us he is trying to get us down but did not succeed guess we got lucky.

/u/patron_saint_of_phishers

Seems like you need thicker skin bub. The mark of a shit leader .. banning people for talking. How gay. Also totally confirms LeChacal is a transgender

/u/Royston

I'd be 99% certain it was World who was attacking ASAP and Dread in order to cause more visitors to go to their scam site.

/u/patron_saint_of_phishers

ASAP is world ..

/u/turbulence0519

Well said. I've been missin dread man! Welcome back, and great job. Sorry you had to deal with shitheads.

/u/yeshello

Can you provide any technical details on this attack? Is it a new method? Simple volumetric attacks on guards? More insight could help pool some knowledge together to strategize.

/u/SE_ExpressSupport

We missed you! Welcome back.

~SankharaExpress TEAM

/u/pedroperuvianus

Please reply to my message. Thanks

/u/SE_ExpressSupport

We will reply soon!

/u/pedroperuvianus

Thanks. Messaged you now with the details.

/u/samadams123

Appreciate everything you do to keep Dread going!

/u/z00per

Welcome back to us. And thanks for your effort and mad skillz.

/u/Preview-Of-Freedom

you sons of bitches you did it. we love you. feels good to be back home.

/u/LifeSucksDie

This pleases me, you're doing a great job! Don't forget to hydrate when you can

/u/IamLegion

I missed you guys!!! Almost got me worried there! A bunch of other DN sites go attacked simultaneously I thought shit was going down, like putin found you guys or something

/u/jonnyfive

Appreciate your work and thanks! Welcome back

/u/Vespair

Welcome back, it was quiet around here without dread.

/u/BigDaddy2K

Good to know guys have been missing dread the past few days!

/u/pharoah P

Damn, I was starting to wonder what I should do with the time I spend every day browsing Dread

/u/Humanman

thank god i was wondering why dread was down!!

/u/gabrieldarko

1 points

Finally online again!

Thank you /u/paris for your job.

/u/desaster

Hello!

Good to see you back here! I was wondering, why Dread was down the last days...But this time, a few sites doesn't works...

I just feel fine, that Dread is back and i can just login...

Thanks,/u/Paris!

Your good work and effort keeps Dread running...

/u/Gladiator P

Good to see you back man :D

/u/daddyDEA

thank you

/u/stormtrooper

Thank you for all that you do! This community is essential!

/u/HighTimesEU

Man those 3 days without dread felt so empty, glad you guys are back.

/u/cannedgoods

Glad you are back bros! Long live DREAD!

/u/Olympus

Welcome back everyone! Think we know who is ddossing everyone. Tried to get us down too.

Glad you guys are back up and running again.

/u/DarkFoxlin

Thank you Paris

/u/rhinarium

Was this attack more formidable than previous attacks?

/u/Natsuko

Glad to see Dread is back! 💜

/u/jethro23

Glad to see dread back up

/u/Grownwithlove

Welcome back! Missed you guys

/u/AuntKateLuv

whyyy whyyy whhyyyyyyyyy!!!! I don't even know what this ddos attacks are :P Is it Russia? feels good to be back home :)

/u/Pragmatica

As a noob... Why do people put money into this, what do they gain?

/u/n0stis

NSA/CISA?
Competitors?
Script Kiddies?

/u/Pragmatica

Competitors, ok. But what does the NSA gain?

/u/n0stis

Dunno. Just asking.

dread going down made news, such as it is, on the Hub.

//Topic: ***What's happening with Dread?*** *(Read 25320 times)*

Takes way too long to load after the robot verification. Most times I get timeout errors.

95% of Dread, seems to be little kids trolling and acting fucking retarded, no offense kids will be kids. I hope this place is better.

This is annoying when you know it's right "You did not answer the verification questions correctly. " But I rather push through 20 wasteful post then ever go back to Dread.

95% of Dread, seems to be little kids trolling and acting fucking retarded, no offense kids will be kids. I hope this place is better.

This is annoying when you know it's right "You did not answer the verification questions correctly. " But I rather push through 20 wasteful post then ever go back to Dread.

Strongly agree, very strange forum..

ZeusMarket
cypjcv237t3qexjou5ciiwxkaaozzrxl2kpexb3lnpwmii7y7vqmctid.onion
ZeusForum
ibm3t6gcptjl7bgp5ufcdb4qltticlhac7s7nofyjmpqix2ylbbhi6qd.onion

Does someone know when registration will be open again?

It looks available now, but I have not tried to actually create an account.

oh nice maybe a bunch of users will flock to this sub like the last time they shit the bucket

Mandatory reading prior to communication attempts. Most unencrypted PMs are trashed.
dread and reddit are living proof of democracy gone wrong
it is in the darkness that you discern the most light
"never liked chasing the dragon as I'd usually end up chasing my own tail" - Beni

Dread is down for me since morning.

Anyone have any idea what is going on?

Dread is down for me since morning.

Anyone have any idea what is going on?

Nope, still down.

NEW SUB KEY AS OF 2022-02-16, PLEASE RE-IMPORT
"Allie often shares the mod crack with me " -T.P.V
"You don't have to be a weirdo to mod here but it helps " -Lucidity
"my wife is a non binary black transsexual amphibious all terrain attack trained doormat i beg your pardon very much
still smells fishy, you better wash behind your ears and other places too"- Benihana
"Anyone who doesn't like pineapple on pizza is a cunt" - Lucidity

>Be me.

>Sees this thread about dread.

>I don't use dread or care about it crashing and burning.

>Comes here to make this pointless comment.

>Laughs at peoples misery missing dread.

>Laughs to self, Fuck dread.

pepe laughing emoji
Those whom dwell in the house of elliptic curves shall forever be encrypted for all time, Amen.
SR1 - BMR - SR2 - Utopia - Agora - Sheep - Evolution - Abraxas - Traderoute - MiddleEarth - Hansa - Alphabay - Dream - WSM

>Be me.

>Sees this thread about dread.

>I don't use dread or care about it crashing and burning.

>Comes here to make this pointless comment.

>Laughs at peoples misery missing dread.

>Laughs to self, Fuck dread.

pepe laughing emoji

it's only the second time around nobody gives a damn, give it time

Mandatory reading prior to communication attempts. Most unencrypted PMs are trashed.

Second? Thought it was at least the forth at this stage

Those whom dwell in the house of elliptic curves shall forever be encrypted for all time, Amen.
http://thehubojcm5xduv2yvoc4tmn5jf4e2hssnlxu66uuknus3jutim7g7ad.onion/index.php?topic=29156.240

More dread speculation

Last week vs. This Week: The Dread Edition

by /u/tekashi6x9 • 1 hour ago in /d/CafeDread

Want to see how badly everyone gags on the fat cock of Dread as if they're an unstoppable entiy that can never be busted by LE

Everyone on Dread last week: "AlphaBay is pushing I2P because it's a govrnment honey pot and everyone knows that I2P is easier to exploit blah blah blah blah DeSnake is obv faking cause he's dead blah blah blah"

Everyone this week: "I just got the I2P launch of Dread set up! So glad to see you guys on there. Way to go Paris. BTW HB has been offline for 2+ months. Lulz. He's probably on the beach sippin right now is all. He's done this before I bet everything is fine. His canary is how many days not-updated? Oh it's fine. Don't worry."sounds a lot like a couple of years ago when Dread went down and Hug's dead man switch was about to release Dread's source code.

Everyone on Dread: "OH MY GOD THIS IT. THIS IS THE END OF THE DARK WEB AS WE KNOW IT. DID YOU GUYS HEAR ABOUT CYBER BUNKER.

https://thecyberbunker.net/ OMG OMG OMG."

*Everyone on Dread a week later after HB played down his absence and Paris "took over": "Oh man you had us going there for a min HB. Thought you was toast. Oh word. Paris got our back. Paris only has a fractionally smaller penis than yours, Hug. But his still must be very large because everything he says is true and he cares about the integrity of this side of the internet just the same as you do. After all, that's what you told us. It must be true. Oh so you're going to take Dread offline for a week for some maintenance? *two weeks later* "Still not online, huh?" *three weeks later* "I knew they couldn't keep Dread down! We're back baby and better than ever! Look at all these cool new features we have and look! Hug even wrote a few sentences about it! Thank god that's over. The Dark Web is safe again thanks to our almighty Hugbunter."*

a few months later Envoy and as well as another forum that I can't quite think of right now for some reason. But basically another OG forum that had been around for ever and served as the main communication hub while Dread was down. The Hub has been the only site other site standing which is not only dead as fuck, but has also been suspected of having ties to, if not completely controlled by LE.

Not everything these fucks say is set in stone. Pretty sure the rule is "act as if everyone on here is a cop". I guess that rule only applies to small fries like me. Read between the lines you fuckin sheep.

- *The Hub »*
- *General Discussion »*
- *Security »*
- *Is it safe to say Dread is officially accepted as finished?*

Author Topic: Is it safe to say Dread is officially accepted as finished? (Read 52 times)

faithlessboofing

- *Full Contributor*
- *Posts: 242*
- *Community Rating: +66/-65*
- *idgaf*

Is it safe to say Dread is officially accepted as finished?

« on: April 24, 2022, 09:54:53 AM »

- *Quote*

After numerous requests and fears of "HB" and "Paris" not properly updating canarys by both users and darknetlive, neither individual has seemed to updated either with HB's experiation at about a month ago, and Paris almost two weeks.

Dread "3.0" lauched with no word from HB - very unlike him to not at least address the community about what was done to make Dread better. I know he's taken a lot of "time off" since his dead man switch activated and put Paris in charge, but now even Paris hasn't updated their canary either.

So here's a hint for any doubters: they're either dead or on the run/in jail. I'm going with the latter.

While I personally believe that Dread has been under the control of LE for much longer than anyone else might think, I don't think anyone can say that something wrong is happening here.

People involced in this business don't sip pina colodas all year round. Like some of you think HB is actually doing. Grow up.

So long Dread. I never fucking liked yout o begin with but it was fun every once in a while.

AND NOW THEYRE PUSHING I2P. Seriously, I dont't know how much more proof you need. It, Is. Over.

New PGP Key. Don't add it. I rarely respond,

benihana

- *Moderator*
- *Jr. Contributor*
- *Posts: 73*
- *Community Rating: +430/-231*
- *reformed troll*

Re: Is it safe to say Dread is officially accepted as finished?

« Reply #1

- *Quote*

I was done with it when the canary expired and so should have everyone else you lose verity and credibility, might as well be greasy donut fingers updating the code since

the push is obvious since they need a foothold in what's to come as well we should reject that iteration, as well always was a cesspool with no credibility

only good thing of it is i2p will see more traffic and people will be able to test its limits further

« Last Edit: by benihana »

Quote from: | Click here to read rules and regulations | on February 20, 2014, 08:28:47 PM
Mandatory reading prior to communication attempts. Most unencrypted PMs are trashed.

T.P.V.

- *Moderator*
- *Legendary Contributor*
- *Posts: 2258*
- *Community Rating: +130/-77*
- *If you're new welcome. If you're lost try Guides.*

Re: Is it safe to say Dread is officially accepted as finished?

« Reply #2

- *Quote*

I2p needs some serious testing as well, it will be a long time before that will be even remotely as safe as tor is.

« Reply #3 on: Today

Allegiance Quote

I never liked that place, to be honest.

NEW SUB KEY AS OF 2022-02-16, PLEASE RE-IMPORT
Allie often shares the mod crack with me " -T.P.V
"You don't have to be a weirdo to mod here but it helps " -Lucidity
"my wife is a non binary black transsexual amphibious all terrain attack trained doormat i beg your pardon very much
still smells fishy, you better wash behind your ears and other places too"- Benihana
"Anyone who doesn't like pineapple on pizza is a cunt" - Lucidity

T.P.V.

- *Moderator*
- *Legendary Contributor*
- *Posts: 2263*
- *Community Rating: +130/-77*
- *If you're new welcome. If you're lost try Guides.*

Re: Is it safe to say Dread is officially accepted as finished?

« Reply #4 on: Today at 12:19:35 PM »

- *Quote*

Yeah I don't think any of us spent much time there.

Then back on dread…

Someone doesn't want us up. April 11 DDOS attack. I2P mirror online?

by /u/Paris A /d/Dread

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

And here I was going to just relax a bit, work on the recon update, and not worry too much. BUT NO. We can't have nice things.

I have been delaying the i2p endpoint announcement simply because my reliability with the i2p network has been... terrible is one word I'll use. It might because how I'm personally connecting into the i2p network or because of how the i2p network system is designed for dread (layers of i2p nodes to the core). I was figuring it out and also gathering information about how the i2p network handles different things. There is a chicken and an egg problem here with i2p. They need more people using their network. It is, from what I got from the IPs and bandwidth statistics on the distributed floodfill nodes, far smaller and far less resistant to Sybil attacks. They don't try to hide that fact (in their fantastic documentation) but it is still a problem. With scale there is a lot of promise here with the proper supports.

Dread will NEVER use any addressbook which can transparently MiTM attack you. It is very important to only visit using the base32 hostname. With that being said I'm going forward with the announcement to provide a hopefully more stable as time goes on i2p mirror.

This is Paris from Dread. As promised we now have an i2p mirror:

http://dreadtoobigdsrxg4yfspcyjr3k6675vftyco5pyb-7wg4pr4dwjq.b32.i2p

It is the biggest dicked i2p website yet. Guaranteed.

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEEbfleES3oPdbct1q5DE1JcU+sN9gFAmJU3NQACgkQDE1JcU+s
N9iFcw//R+h7ppmmvpjLh90qOdRmzTxC4x5SjXSThBN3Am/+AWY8XJX+tJ1wSlMj
KxzsOWyfZ/Tr4sOBvvSNK975oMvN4WlxEmYg0cd5Nvz1z/Q0sS3uYQrwociuS4Vk

LspqyL3N+wiTwySwGci2JxzQexPbt9sEIDo9haIFbsVHXsVMD4ZpsvmgGd
dl07UJ
QxF7YmVshnImNcw4eYVUNtCim+586ldJPYyGdciBUgRRbGLZE0JTTQ3
LcGZ3Wk2w
YDXcQ1D6DaYmRHFnntxS2G3Q4TSG+KuJwak7ZAbC31fU2QrG+EmT3K
Rjhw7jpPDR
Hieyib/2tjwNcpfnigvWdJIN3AW4JMtW9Q/DKtZt3oBeZtBdirInUZadRps
MitCy
dpsYoftAnDW96UC13uTH+RQWVUAtJcuByuCOaJWRrxeD/cQdbYwAf7Et
GEVED6HR
vnkicwaJCWGtd5fN8jYUhIA0a93qEcujJnQcvYlJjvXUvdeKNO4BXnOlsqg2
0WSd
iBVdFQfdVr3lX/+UjkmS9/ZmsDELiNDg/iCGGg4SWgWQC+dNcldRqSp3
fZw4R6v5
yk3hfdBMRCNcyPsUVYflSt+aBD+46G6nN5FRfi8Lw/CTdmVgveR+lk+gSd
J5P1+k
OlgM3ppCwjA7wp9vsfam5jgnUz7b6mhtPhnp0kQ+zyC7R3QdKDg=
=FxQf
-----END PGP SIGNATURE-----

/u/makemecry

these were ~24 long hours without dread, i realized i'm addicted to it.. should i get some help?

/u/ATOC

Good work on the i2p link.. is working decent, stable on i2p - Good to be back

/u/BCKM

Tremendously helpful and necessary forum, Was indeed worried for a bit. Glad we're back up and running.

/u/PaperHat

Been using Tor for 9 years but have no experience with i2p. Would someone kindly explain the pros and cons of i2p and Tor?

/u/123doerayme

same..

/u/ShulginIsMyGod

NOICE

keep it up! (I mean... really lol ahah)

/u/user0001

Good job Paris! I love that i2p mirror

I'm proud of you

/u/ProfessorsEmporium

You gunna need a wheelbarrow for that thing!

/u/chagamushroom

Wen i2p for tails?

/u/cannedgoods

When Dread back on TOR serrr?

/u/daddyDEA

soooo, dread and abacus main mirror on same server location?? See you soon son.

/u/Papinian3

Dear Paris! Welcome on I2P board (among us)! What to add? Stay ahead of the game! ;-) Rgds. Papinian3

/u/luvu3

You are doing the lords work Paris.

/u/LoveMeSweet2022

far smaller and far less resistant to Sybil attacks

That was what Bazil Fawlty used as an excuse every time he used Manuel to be the barer of bad news to his wife

/u/fishgender

TYVM!!! I'm a big big big fan of I2P. Can't believe it has arrived!

/u/drakoflako

i am using i2p right now and like it, well done so far!!

Java alert appears very often..

But at all, great project, keep it up! Thanks a lot =))

What happened to the I2P endpoint promised on Dread v3?

by /u/fishgender • 1 week ago in /d/Dread

I found a dread.i2p domain registered on reg.i2p, but it has never been online. On the launch post of Dread v3, it was promised that I2P endpoint will be released within a couple of days. It's been a month. What happened?

/u/daddyDEA

we are setting it up as we type

/u/fishgender

Thank you! Currently commenting using the Dread I2P!

Then even more on Envoy

qubes_fiend76

- *Newbie*
- *Posts: 3*
- *Penis Size +0/-0*
- *Your mom goes to college*

Re: I2P or Tor

« Reply

- *Quote*

Even though DeSnakes over-confident statements on I2P over on Dread are fairly annoying, I2P actually is the better and safer anonymous network to use...in theory. It would be, if it was as huge as Tor has gotten. The biggest weakness in I2P is the small user base, which is just common sense: to a global three letter adversary that can monitor very large portions of the internet at a time, the fewer users using "garlic routing" (I2P's answer to 'onion routing') the easier it is to conduct traffic analysis.

In my opinion, I2P's routing protocol is superior to Tor's. The encryption is more...encrypted-ey?(sic). And the decentralized nature, where every user is a node (instead of Tor's centralized and public node list anyone can download) is why I would pick I2P over Tor any day. Plus I2P was actually built to be a "darknet" whereas Tor's primary function is obfuscating clearnet traffic. Don't get me wrong, there are still downsides to I2P (small user base, more difficult to setup for some people, lack of stream isolation requiring you to restart I2P alltogether if you want to visit more than 1 eepsite in a single browsing session and avoid fingerprinting/traffic analysis attacks, etc), but i find that list to be significantly shorter than Tor's downsides.

I2P has the potential to completely change the darknet game if more people would jump on it and learn how to use it properly and safely.

BTW, i suggest browsing the github profile of one of the creators and maintainers of I2P. go to github, search "eyedeekay" and you'll find his profile. He is all the time tweaking and updating and creating tools to make the network more accessible for everybody. You'll even find repos and scripts for dedicated I2P browsers or all-in-one installers. Good shit, man.

- *Envoy » Cyber Insecurity » The Onion Router » The Garlic Network » I2P or Tor*

Then a week or so later this topic continues under a different message thread on dread. A complicated thing, keeping these sites up. Not for wimps. A deadman? Really?

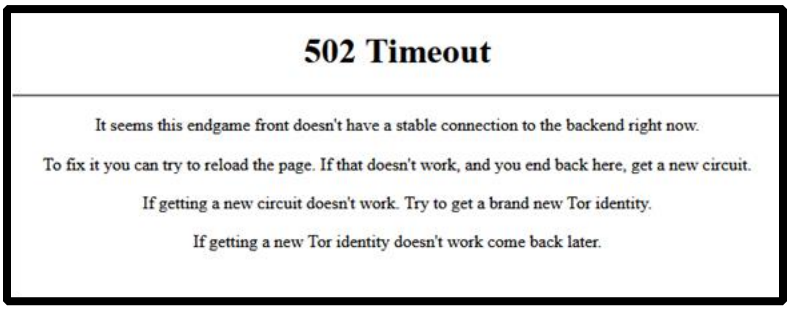
And we are back up again

by /u/Paris A • in /d/Dread

After a few hours of troubleshooting the 502 error thinking it was the database dying it was just in fact a bugged out internal DHCP service handing the wrong IP to the load balancer. Problems with cluster moving.

We should be solid again. More adjustments are coming to provide a bit better performance. If we go down we will come back just give us a bit of time to get

things sorted out.
All ads have been extended/refunded.
/u/Raphaeliouz
Glad to hear it !
/u/Jinba
I just downloaded i2p when i finally figured it all after 1 hour it opens on regular tor nice
/u/snowpiercer
good job man...
/u/capobianco
Aww I really liked the i2p dread website :(but its great that dread is back and running !!!
/u/Paris A
The i2p endpoint is still online.
/u/Pixels
finally, after all day long cuddling with 502.



Note: 502 Bad Gateway Error. A 502 Bad Gateway error indicates that a URL request or attempt to visit a web page returned an invalid response. Bad Gateway errors are often caused by issues between online servers that you have no control over, like misconfiguration or DNS problems.

Who create / admin server of dread? and why is not open source
by /u/Ankhknight in /d/Dread
Dread works good similar too reddit but there's some question about how it initially worked
Why is not open source code?
There's some mobile apps using tor, why not dread app?
/u/yossarian

/u/Paris mentioned somewhere that there's a dead man switch which will release the source code of dread if something happens to both /u/Paris and /u/HugBunter

/u/Paris A

We don't want people to use their phone for accessing the darknet. There is far too much information capture and personal information on people's phone. It's horrible for opsec.

/u/hugbunter created Dread. It was planned to be open source but the code is far too complicated with tons of proprietary systems for anti-manipulation which is far too hard to remove now. In the case I am compromised and my deadman goes off dread will redirect to a read only git.

Note: *A deadman's switch, as explained by one Dark Web marketplace administrator, is a type of security system that is put in place to ensure the individual who set up said the system is functioning properly. This sounds very dramatic, like something you would see in an episode of Mr Robot but they have various uses as we have seen with both Edward Snowden and WikiLeaks where if a predefined step or measure was not taken in a predefined amount of time files would be sent to a predefined location. It doesn't always refer to the living status of an individual or being but the fact that if that person is not freely able to essentially flick off the switch something will be triggered.*

https://darkweblink.com/paris-reveals-that-hugbunter-deadman-has-switched/

What is the git he refers to?

GitHub

GitHub, Inc. is a provider of Internet hosting for software development and version control using Git. It offers the distributed version control and source code management (SCM) functionality of Git, plus its own features. It provides access control and several collaboration features such as bug tracking, feature requests, task management, continuous integration and wikis for every project. Headquartered in California, it has been a subsidiary of Microsoft since 2018.

It is commonly used to host open-source projects. As of November 2021, GitHub reports having over 73 million developers and more than 200 million repositories (including at least 28 million public repositories). It is the largest source code host as of November 2021.

https://en.wikipedia.org/wiki/GitHub

And then this appeared:

DDos Attacks

What can be done about markets facing DDoS attacks?

by /u/mommy /d/CafeDread

I hear most of this happens due to market admins attacking competing markets. This makes sense, but there has to be another way, right?

Is it not possible for some of these market admins to work together in some way where everyone benefits?

Aside from that, is there not a better way to protect against the attacks themselves? Plenty of these people seem to have the funds and expertise to do SOMETHING more, right?

I could be wrong, but it's just annoying that tons of customers have to sit around waiting before they can even get a chance to throw more money at markets/vendors because there's some darknet slapfight going on every other day. No hate to any admins, I'm sure they deal with a lot of bullshit, I just don't understand why this issue is so prevalent.

/u/merlin P

As a competitor it is impossible to work together, as for ddos attacks, no matter how hard you try to protect, there will always be new ways to attack ddos, there are many ways out there.

You can try scale the transit capacity/server capacity, but even so it hard until the end to protect 100%

/u/Papinian3

Then you can try to connect via I2P market mirrors if there is such possibility. Kingdom, Alpha etc...

/u/BellaStar

There are certainly some market admins that have friendly relations with each other, but clearly there are also others who are bitter rivals. In the early days of the darknet there were reports of some admins facing ddos attacks simply from people trying to force them into paying ransoms (and allegedly these were even paid on occasion - something that's unlikely to happen today).

There are signs that markets with sufficient resources can out-scale and/or mitigate against ddosers though, as appears to be the case after the recent downtime of ASAP that now seems to be working just fine again after their upgrade.

It'll forever be a game of cat and mouse unfortunately. That's just how the darknet is...

More about DDoS on dread:

Targeted DDOS

by /u/HappyPancake69 in /d/CafeDread

I may be an idiot asking this, but.... Why are all the markets despite Alphabay being DDOSed?

/u/SloMoSide

yes.... exactly.... WHY ! ! ! !

/u/DeSnake P

Because we are more technically capable than the rest and we took our time to build the firewall to defend against DDoS attacks (in the beginning we were attacked every single day all the time for months on end). We get attacked now and then but they see they make no difference hence they stop after a while. ***It also costs us peanuts compared to what the attackers spend making it even less economically viable to launch attacks on us.***

Thank you.

/u/7664r8

how does a firewall for onion ddos work for layman? i thought you always have to outspend the attacker. why are you the only one who can do this firewall while dread burns through cash to stay up? is it rate limiting market functions

/u/DeSnake P

I have offered to help them but Paris does it with his own method.

Usually yes outspend. ***That is if you are stacking horizontally endgame instances.*** *I can not be specific about what we are exactly doing to achieve effective protection on the cheap. But best I can give advice to other operators*

is to read their error messages everything they need to do is right there. Couple that with Linux administration experience and some weeks of testing and they can get a good firewall like I put together for AlphaBay. Thank you.

/u/Grazelda P

Keep in mind that claiming a DDOS attack has grown to become the #1 go-to excuse for any site problems. Instead of "had to rebuild a corrupt database" or "we fucked up the code" or "oh fucking oooppps" it becomes "DDOS ATTACK!" and suddenly gains sympathy. Not saying that DDOS attacks do not happen (they certainly do) but that excuse seems to have become a panacea for damn near any site operational problem. And you cannot blame any site manager for not disclosing their backend tech. Sad because I find DDOS defense techniques to be fascinating.

Sadder still is when a site actually works and you get your DDOS defense tight as hell -- accusations are made that 'they' are the source of attacks. Its all just FUD spreading without proof.

More about IP2 on dread:

Having a backup is important, don't get caught without one!

by /u/Paris A • in /d/Dread

The amount of request for PGP purging on Dread because user's forgot to backup their PGP is far too high! If you don't have a backup, you should make one right now. While we are talking about backups, due to the rise in DDOS attacks, you should all also have a backup of Dread URLS.

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Dread's URLs are:

Tor:

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion

I2P:

http://dreadtoobigdsrxg4yfspcyjr3k6675vftyco5pyb7wg4pr4dwjq.b32.i2p

Signed by /u/Paris's PGP key

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEEbfleES3oPdbct1q5DE1JcU+sN9gFAmLDj+0ACgkQD E1JcU+s

N9js2w/9GWLKhsx9WNT4HwvHrdki35/7xFypAsnEEaLtDMoe94ERm1+ec M8EZHiR

5kPMfSejqvTP5tL/HlLcrQM0H2soz5o/HoN/swez5t3LlCwwr1e2H+SCDvgr XKNi

y4KxevySJtvTxMtd2C8grUHtS+JNDFOS6vlmsapyey3/kKd9KFIzYqo8V04 73N0B

0gGAVBQzX+GJup4u0Vf+TxyB2ELDZIY7L7GwNCxjhif2lPanS6LHe9Joro5KhkGR

YVWJcgwz7x7m0e7EqCqEeOITt4qIn3wkAAHb7S8rqkcg4SrFUvuwlkUss+l3RS6g

plv3oVQtsh6kJ9rAhgmUOBrLY8oBxxPmZSUQYmcXtAQes13pfSY9lwFKkPDvmT4H

nxK10oh3h+gO2Z0c9FYeUn7VNY/MFQoZfYBAyiFn/i32UJj2fuuK8Wju0fIoYS63

ykV0zniiqdn3kwL1VEk6X29DJZGgIRfb4WyZs4XjaQZyFD32PecfsnixEQRQl+z+

pYdo+niY/tPNKdOzxLCfHOBj6cVCmdRSAz0chfozo4pF79mm1edLBHKi2XxEcXfq

pCiu/rLb2fKwJOYHEMxWuAkRx+UBx3TvdlojOyuqrxWWa4tZ3PlicjXQCS9wqFo9

DJyeRaEjQg+AT2uv0TrbFZvPhJLood6Xkg53vWHkZdThmIsaixY=

=7RuG

-----END PGP SIGNATURE-----

Dread is accessible both on Tor and I2P. Being that the attacks are all on Tor's hidden service side this post will focus on how to get setup on I2P the easy way. The vast majority of people who visit Dread do so on the Tor Browser. Did you know there is a I2P browser as well? It's true. https://github.com/PurpleI2P/i2pdbrowser

Getting setup is super easy! You can go to either the releases section to grab the latest version or compile it yourself if you are inclined (for non-windows versions make sure to update the build script firefox version). If you are on windows the fastest way to start is download the .exe version, run, and extract to a directory. You can then boot it up just like the Tor Browser. That's it. Due to how the I2P network works the longer you use it the faster it becomes for you. So it might be slow at the start but if you give it an hour or two it will start to load faster.

Best part? No EndGame captcha on Dread's I2P version. Plus with the forever cookie set you won't need to sign in again if you do close the browser. It is far more convenient.

There is a warning though. I2P's network works completely different from Tor. When you are on Tor you only directly connect to a small amount of nodes. Your request goes in and a request comes out. This means your surface area to those who know you are connected to Tor just the authority servers (you get the descriptors from) and your guards. You are a user of the network but not apart of it. I2P has a different system that is closer to P2P torrenting. This has a lot of benefits but also some drawbacks. Unlike Tor which tries that mask you are using Tor (bridges, limited guard nodes, and all that) I2P does not

hide you are using I2P. By running I2P on your system it becomes apart of the I2P network. If you don't want people to know you are using I2P you need to proxy it locally from another server or use a VPN. The network is completely distributed and self organizing. It is specifically designed for hidden service connections and can be much faster and more resistant to DDOS attacks assuming equally high participants and capacity in the network. By running I2P you are increasing the network capacity and resistance to attacks. Unlike Tor where the more users creates more drain on limited network's resources.

I did the math today. If just under 10% of the users on Dread daily ran a I2P server we would have a larger footprint than the totality of the Tor network. That doesn't mean we would have the same capacity but due to the reduced load on the I2P network, compared to Tor, the connection would be more reliable and likely much faster. There are a lot of benefits to it. Give it a chance just to check that the backup works as planned if the Tor site goes down.

56 comments

/u/Paris A

9 points

I2P usage is up over 500% after this post!

/u/LeeYoo-Mi

1 points

4 days ago

i2p is been around for quite sometime now but normal users hardly use it so having something like i2pdbrowser could change the whole perspective towards i2p

/u/BlackMarketplace

1 points

Yeah, I2P has been around for a long time.

It's just that people, don't want to step out of their comfort zone.

Just like people, in the beginning, didn't want to believe in BTC.

/u/mrbenzo666

1 points

or how ppl still use btc over xmr lol

/u/zexdac

3 points

Thanks Paris. I verified my backup restores successfully, saved those links, and am running a I2P server.

/u/clipmip

1 points

> I verified my backup restores successfully

This is super important. Gotta test those backups!

/u/Lollyb99

2 points

Alright, let's give it a crack.

/u/byballotbybullet

2 points

Unlike Tor which tries that mask you are using Tor (bridges, limited guard nodes, and all that) I2P does not hide you are using I2P. By running I2P on your system it becomes apart of the I2P network. If you don't want people to know you are using I2P you need to proxy it locally from another server or use a VPN. The network is completely distributed and self organizing. It is specifically designed for hidden service connections and can be much faster and more resistant to DDOS attacks assuming equally high participants and capacity in the network. By running I2P you are increasing the network capacity and resistance to attacks. Unlike Tor where the more users creates more drain on limited network's resources.

So what's the OpSec risk with using I2P?

If they know I accessed the I2P network, can they know I went to a market selling drugs?

I remember using torrent and ISPs would know exactly what movie you downloaded and would send you warning about where you went and what you downloaded as a deterrent (I always threw them in the trash and continued on).

But illegal drugs feels just a bit...actually a LOT more risky to run across a torrent-like protocol.

Or is this unknown? Kind of like all the lessons learned from the beautiful disaster that was Silk Road and AB-1. We laugh now at some of the fails, but how could they have known? Being ahead of the times also means being ahead of the knowledge (much of what could possibly be known to be good or bad).

/u/xrbuzz

3 points

If you're going to run I2P I would do so only over a VPN router at the bare minimum.

I wouldn't trust I2P unless they add the option to connect to a remote I2P server over Tor, it would be ideal if Tails supported a I2P over Tor via remote server, thats the only situation in which I would ever use I2P.

/u/byballotbybullet

2 points

well, main issue seems to be the unencrypted log files stored by I2P router on local device that can lead to discovery of user or their browsing habits. a VPN wouldn't prevent that, though it might delay you getting raided (since no VPN provider will likely stick its neck out for anyone).

/u/cannabliss420

1 points

That's why many darknet users use Mullvad. They have no obligation to comply with US authorities.

/u/Paris A

3 points

I2P has similar privacy guarantees to tor. When communicating on the network it's designed to provide privacy. They won't reasonably know you are visiting anything at all. There is in fact a larger guarantee when on the I2P network of that fact compared to Tor. Because in the case of your connection is being monitored they would see not a direct line between one or two peers but many many short lived connections over many more. The way ISPs knew you were torrenting a movie is that copyright holders monitor popular torrent sites and torrent links and record who connects and starts downloading. This is because torrenting is a open IP connection where everyone knows what the others are doing/have. I2P, by it's design, protects your privacy while on the network. So while it is similar in it's connection process for peers what people know is far more privacy oriented.

The OPSEC mistakes from many major markets are mostly not because of the networks people use to connect to them but the market application software or admin mistakes in building/marketing the market. It's an arms race and people need to understand there are risks but with reasonable processes and common sense they are manageable.

/u/byballotbybullet

1 points

Sounds great. And the convenience. If it's as robust as you say on the privacy side, and this can be done from a Windows OS, then wow. The DN might be poised for a serious boost if more DNMs (think it's only AB so far?) offer services on I2P.

Btw, does this mean these vulnerabilities are no longer relevant (the issue of unencrypted log files stored on the user's local system especially - the phishing attacks are an issue everywhere, so I disregarded those): https://www.tandfonline.com/doi/full/10.1080/21642583.2017.1331770

/u/Paris A

3 points

I2Ps domain resolution system is problematic. The .i2p domain problem is still there and the way it's design makes it impossible to fix without completely changing how it operates. This is why we request everyone to only use the full address and not an address book (which could come from a compromised registrar) that could MITM attack. If you use the full b32 address it has the same connection guarantees that onion services have.

Seeing if you are running I2P is obvious to an outsider. They do a poor job of masking but that is more so a product of the network design (where you are apart of the network not a leech off it). This is why if you care about if people know you are running I2P to use a VPN or to just proxy from a remote server.

All other problems with the network are mostly a product of the low latency design and are shared with the Tor network.

/u/enosh

1 points

I have actually been thinking of doing this with my pgp incase my "burner" laptop dies. Just not sure really where to start. I am most definitely a pgp newb. All I did was researched he basics of pgp years ago just to be able to use the markets. When I downloaded GNUpg/GPA and I remember it asked me to write down my "SEED" phrases and to store it in a safe place offline (along with all my other important passwords/phreases/mneomonic keys). I did that, but I actually dont know what I would do if my whole system crashed. I mean, I imagine I would download the same program and I would be prompted to enter my seed? I am not really sure. What is entailed in backing up ones PGP? Do I need a backup of my key ID and/or my fingerprint? Any info would help from anyone knowledgeable in this area. Thanks!

/u/newbieforever2018 ☆Cares About Noobs☆

1 points

I don't use the same program that you do but I have a "manage keys" choice. From there I can put a check in the checkbox next to my key and then choose "export to file" and save it wherever such as a usb or external drive. My program also has an "import key" choice so I could reinstall the program on a new device and import my saved pgp key.

/u/enosh

1 points

Ah yes, I see where I can import and export key for my program. When I tried to export it prompted me to save a file. I saved it then when I opened it it was just a copy of mt key. Now mt question is: on my key ring, I have all the saved "public" keys I use, and then their is my key that has a "public" key and a "private" key to it. So when I exported my key, I imagine that is just the "public" key for others to encrypt to me, but how do I know I am also exporting the "private" key that I use to decrypt?

/u/newbieforever2018 ☆Cares About Noobs☆

1 points

My bad. That is indeed how to export the public key. My program is portable and I just save the entire folder periodically which saves everything.

/u/newbieforever2018 ☆Cares About Noobs☆

1 points

Thanks so much for this topic /u/Paris

At the risk of admitting to being a Windows user what is the difference between the windows and windows_prebuilt versions of the web browser for i2P?

/u/Paris A

1 points

You will need to use the windows version not the prebuilt. Prebuild is for combining everything together into an easy to send exe while everything else needs to be built on a user's computer.

/u/newbieforever2018 ☆Cares About Noobs☆

1 points

Okay, thank you for the response.

/u/TrippyHippy

1 points

I finally went out and bought a usb to make backups of all my important info not too long ago. I was one of those users who messaged requesting for PGP purge. Now I need to go get another usb to make a extra backup of that backup.

Also barely today was looking around into I2P and I did not know there was an I2P browser! I still haven't messed around with it too much and don't really know much on how to navigate it so hopefully that is easier with a browser.

/u/TZSKSKTZ

1 points

SD cards are great for backup, discreet, and cheap

/u/solingen

1 points

What is the recommended use of the I2P browser opsec wise? I am using Whonix - should I install the browser on Whonix or is it safe to use on the hostOS/other VM instance?

/u/bleedinirish

1 points

Thanks Paris.

Kind regards

Thatirishbloke.

/u/Paris A

1 points

Use it with a VPN or proxy the I2P process from another server. Using with whonix wouldn't be possible. I2P requires direct connections for stability. You can run the browser in it's own sandbox or VM if you want. Depending on your risk tolerance.

/u/MommyCrush

1 points

"Using with whonix wouldn't be possible."

Just fyi, I2P does work with whonix. The original java client is awful but my workstation runs I2Pd beautifully. So even if there are flaws in their network we have not discovered yet, I'm still protected by TOR (:

/u/Paris A

1 points

For stability I highly recommend not doubling up networking. Think of it this way. In the case the Tor network crashes, your I2P connection would also break up. You also would be proxying over more hosts with a direct connection point of your guard node. That removes a lot of the privacy guarantees I2P provides to people from their shortlived connections. It's just a bad idea.

/u/ned7887

1 points

I'm confused. I'm following the I2P guide on AlphaBay and it specifically says to run the code to set up I2P on Whonix/Debian flavours.

Am I doing something wrong?

/u/Paris A

1 points

Running on Debian is fine. It's going to be far faster and more performant using the Linux kernel. Whonix is built on Debian and is counted within the same distro flavor. That doesn't mean you should use I2P with whonix and proxy all your I2P connections over Tor.

/u/UnKnOwN8733

1 points

Works great, thanks. Is there a list of available I2P links somewhere?

/u/Paris A

1 points

http://reg.i2p/all

/u/flowerbuyerunit

1 points

Good reminder. One should have back up for each steps.

/u/DrSwole

1 points

For a user using Tails how would recommend story the backup

just a straight up copy of Keepass database and keep off site

or do a full second install of tails and move everything over. Then youve got the benefit of FDE?

DOC

/u/xrbuzz

1 points

Dude, there is a back up utility in tails already built it, use that...

/u/ned7887

1 points

From AlphaBay 'How to' guide.

'We HIGHLY RECOMMEND using I2P over Tor for many reasons which you can see in Frequently Asked Questions (FAQ) section. Currently Tails DOES NOT work with I2P and requires too much configuration for the average user to do on each boot. We are working on Tails having I2P/custom script for Tails'.

I'm a noob to all this and all these conflicting messages are very confusing.

/u/azfphree

1 points

have been running i2p for a week or so, can confirm dread loads great. almost never any downtime and love that you get to bypass annoying but understandable access queue.

maybe you can add a sitewide msg encouraging users to make the switch to i2p?

/u/Paris

/u/Warningo

1 points

Good reminder and thanks the infos

/u/dayaftertomorow

1 points

Nice Explain

i just downloaded it and its workin fine !!

thank you

/u/Zergburgers

1 points

Let's say I have a pgp key on tails. How can I back it up if my usb does? I don't even understand how I would be able to transfer it to another usb stick, for instance.

/u/patron_saint_of_phishers

1 points

This is refreshing to see after years of bashing I2p. Garlic routing is far superior to onion routing and have been saying it for years, welcome to becoming an I2p head.

/u/Paris A

1 points

Their Java client is shit still. But i2pd saved them in my mind.

/u/spiltnsplit

1 points

So, you can use i2p over tails, correct? And if it's safer to use a VPN with i2p (unlike Tor), then would using the hotspot on your phone as your wifi conncetion on Tails be secure as long as your phone's wifi is using a VPN?

Or would there be a safer way to do this such as not using a cellular hotspot, regardless of a VPN??

Thnaks for your help!

/u/armatek47

1 points

Unfortunately just learned that i2p isnt supported on tails anymore since 2.1.

/u/SmooLack

2 points

Lame...

/u/armatek47

1 points

They are looking for a volunteer to take care of i2p in the next version tho, crossed fingers.

/u/bhandaatma

1 points

Learnt it the hard way :(

/u/greenRC

1 points

Which other Markets Can I sell My fire Crystals Analogue (Eutylone, MDMA) AS We have Warehouse in USA.

Besides, alphabay and ASAP

/u/anonchansama

1 points

I2P to the moon!!

/u/toprakzdigaz

1 points

Top information yes bro!

/u/methSavoy

1 points

Backups are very important. I always make sure to have a copy at least two

times on two different places.
/u/House81
1 points
Thanks for your hint :-)! Is updated now.
Greats
House81
/u/hp_617
1 points
Thanks, made backups!
/u/Scarface_Alpha
1 points
Great info for those who don't know much.
/u/kcats
1 points
Bad things happened to my hardware after downloading i2pdbrowser

Then n0stis got this message on dread:

You have been banned from this community.
A moderator at /d/vendor_handbook has banned you until: 9th June, 2032
Reason: Offensive behaviour

Wow! Only ten years? I never even posted to this sub. And then followed by this message:

You have been banned from this community.
A moderator at /d/SpiritualHealing has banned you until: 9th June, 2032 -
Reason: Offensive behaviour
Ok, so this one I understand. You didn't like being told to pull your heads out of your asses, I guess.
This banning however is way worse than reddit and really unsupportable in a venue that supposedly supports free speech.
/u/Pygmalion
1. Free speech does not apply on a private avenue.
2. Calling people names is a poor use of your free speech.
/u/n0stis
Well, I didn't actually do any name calling, as I am personally opposed to that.
What I did is describe behavior and give a recommendation for Cranium-Rectal inversion therapy.

This British spelling perhaps reflects the server being hosted in a British speaking country. No stiff upper lip here I guess.

Insider Story Two </html>

Designing the perfect encrypted communication tools

/u/Hugbunter, /u/paris, /u/solar, and /u/matter, with /u/wintermute, /u/syntax, /u/Shaky, and /u/Cyberjagu being too camera shy to pose

- ***Second Goal: We will modify the Dark Mail email software to more fully integrate it into the RealOS, as well as upgrade the level and type of encryption, improve the PGP encryption/decryption engine to support html (rich text) fonts as well as graphics. No small task in and of itself.***

/u/hugbunter, /u/paris were working with The Dark Mail Alliance team consisting of Phil Zimmermann, Jon Callas[43], Mike Janke[44], and Ladar Levison[45], to make all email surveillance-proof, i.e. secure by default.

---

[43] Jon Callas is an American computer security expert, software engineer, user experience designer, and technologist who is the co-founder of the global encrypted communications service Silent Circle. Prior to this he was co-founder of PGP Corporation.
[44] Mike Janke is a founder of Silent Circle, the world's leading Global Secure Communications service and the makers of Blackphone - Time Magazine's top 10 invention of the year.
[45] Ladar Levison launched Lavabit in 2004 on the principle that everyone —individuals, organizations and businesses—has the innate right to private, secure communication.

For the second goal:

We would continue to reverse engineer the MS Outlook client, adding importation for PGP keys, and ability to interoperate with Tor addresses and encrypt/decrypt seamlessly. We aim provide a secure communication platform for asynchronous messaging across the Internet.

Their moto became Meet Dark Mail" we are planning to Keep the NSA Out of Your Inbox and we need to make it auto-magical in terms of ease-of-use.

When you send an email it would ask Clear text or encrypted and at what level? Then ask you which PGP key to use.

When you receive an email, it would be automatically decrypted by your PGP key. The recipient would simply need to import their keys to read and send.

Encrypted messages in your In, Out, and Sent boxes would be marked as green to identify them as such.

You could send your public key with your message, or send encrypt invitations much like Outlook Calendar invitations now.

You would import your existing keys at installation.

Anyone monitoring the email would be able to see the size of the message but that is about it. If sent over a Mixnet, not even that will be seen.

Dark Mail will use a newly developed messaging protocol, which is designed to provide end-to-end encryption of both the message itself and the email in transit. Because encryption will be integrated into the protocol itself, it will be invisible to the user. Dark Mail users will get the security of PGP without the cognitive burden of manual encryption. Anyone who can use email today will be able to use Dark Mail.

The group agreed that we now needed a MIL-SPEC[46] cryptographic email system for the entire planet just to be able to talk to our friends and family without any fear of government surveillance. So we need to do their encryption on the user's device where the encryption keys stay, and where no one else ever has them.

One challenge of creating encrypted email that the group recognized is that managing encryption keys can be difficult, for the not-technically-inclined. Zimmermann and Levison will help us to design Signets, which operates similarly to the public-key system of the well-known email encryption protocol PGP. Signets are user profiles-slash-key managers, named after signet rings used to seal letters by making unique marks in sealing wax.

Users can reveal their Signets to those with whom they wish to communicate. Signets will contain a unique cryptographic signature used to ensure a message's authenticity.

In some ways, DIME will work like Tor, the networking protocol that anonymizes Web traffic. When data packets move through the Tor network, the packets' headers (addressing information such as sender, recipient, etc.) are partially encrypted, so that no one relay knows everything about the packet's origin and destination.

Email sent through Dark Mail will take a similarly segmented route, so that only the recipient and sender will be able to see the full contents of each email's headers.

Dark Mail will take the extra step of cloaking your email's metadata, which includes the subject line and the 'To' and 'From' fields. That way, spies cannot easily identify who is sending emails.

But for all its complicated encryption strategies, Dark Mail will still rely on the most basic of security tenets: a strong password.

"If your password is 'password,' nothing we do will save you. Encryption will be as strong as your individual passphrase.

Metadata cloaking important? Even if the NSA cannot read the body of your message, knowing whom you email can trigger extra government scrutiny.

The NSA uses email metadata collected on millions of Americans to select specific people for closer surveillance of emails and phone calls. So consider that for every one target, nine of their connections are spied on too.

---

[46] A United States defense standard, often called a military standard, MIL-SPEC", is used to help achieve standardization objectives by the U.S. Department of Defense and three letter government agencies..

The NSA's bulk collection of metadata should remind us all who are old enough, of the guilt-by-association of the 1950's Communist-hunting McCarthy era.

This indicates the loss of the freedom of association, and that if I email you, and you are under surveillance... I will, in turn, place myself under surveillance."

Dark Mail is not NSA-proof. The government can still target a person and follow each email's trail. But to do that, the government would have to trace every stop along an email's path -- device, server, server, and device.

Using Dark Mail is like mailing an envelope that, on the outside, is only addressed to and from post offices. Finding the actual sender and recipient is not an unsolvable mystery, but it creates some drag for the dragnet. Dark Mail should make it technologically impossible to conduct mass surveillance.

Dark Mail will work as an add-on with all major email services -- as long as they make slight tweaks to their code. The Dark Mail Access Protocol—DMAP—and Dark Mail Transfer Protocol—DMTP—will need to replace IMAP. The Dark Mail reputation system will filter out unwanted & un-trusted email.

Meanwhile, so back to the goal of taking down Facebook, the irredeemable evil corporation which is predatory on human beings and a parasite on our society that, if left unchecked, may very well take down American democracy and facilitate a civil war? No small task.

There are 20 US Facebook data centers and 18 more worldwide, 13 of which are currently serving traffic. They all have occasional outages

A typical Facebook datacenter

Founded in 2004, Facebook needs no introduction as the world's largest social network. All the status updates, family photos, and videos add up and create a need for a massive amount of storage and compute. Facebook maintains a growing stable of data centers spread across the world.

Massive storage for stolen personal data is what they actually mean. A single datacenter can be one million square feet and a single Facebook data center processes 10s of terabytes of traffic per second, draws 10s of megawatts of power, and runs thousands of software services, serving more than 3.5 billion active users and 2.76 billion daily active people.

The data centers include massive facilities with millions of machines and smaller facilities that connect the backbone network to the broader internet and people using Facebook's platforms.

The data traffic between all these computing facilities is managed by routers, which figure out where to send all the incoming and outgoing data.

Nebraska Sarpy Data Center
Texas Temple Data Center, Fort Worth Data Center
Ohio New Albany Data Center
Georgia Newton Data Center
Oregon Prineville Data Center
Idaho Kuna Data Center
New Mexico Los Lunas Data Center
Arizona Mesa Data Center
Virginia Henrico Data Center
Alabama Huntsville Data Center

Missouri Kansas City
North Carolina Forest City Data Center
Tennessee Gallatin Data Center
Iowa Altoona Data Center
Illinois DeKalb Data Center
Utah Eagle Mountain Data Center
DNS server computers at the Santa Clara, California, data center

Thumbs down and not up for us

The goal was to first introduce the malware to each datacenter while simultaneously taking out the DNS server network to contain the malware and not expose the outside world. By not having BGP announcements for the DNS name servers, DNS falls apart which means nobody can find you on the Internet. We will kill all US datacenters simultaneously and permanently to make sure Facebook never celebrated a 20th Anniversary.

Unlike the infamous 2012 Saudi Aramco Shamoon hack[47] we will not ask for a $50 million ransom for 1TB of data, nor allow a relatively quick five month recovery such as them simply ordering 50,000 new hard disks.

Since the Facebook systems are designed to audit command to prevent damaging errors, the malware will also place a bug in their audit tool to prevent it from stopping the new malicious commands.

A plan started to take shape that we would use the corporate money making, personal info rip-off IOT devices against them for major

[47] *https://en.wikipedia.org/wiki/Chris_Kubecka#Saudi_Aramco_security_work*

DDOS attacks against each center. We would then slip in software (malware) to erase every machine, destroy it and brick or door stop all their backbone routers that coordinate network traffic between data centers disrupting these communications. There would be no easy recovery allowed.

These IOT devices (sensors and actuators actually), like thermostats, doorbell and surveillance cameras, routers, etc. typically do not have enough memory in them to set usernames and passwords. Even if they do, they are typically left to the default settings by the owners, like Admin and Admin.

In addition, they will hack the 100,00 or so EV charging stations in the US, *nearly 140,000 Wiseasy payment terminals around the world* and add them to this malicious bot net.

Their email and phone services would not work either, because those also go through their network. And again, no network traffic means no communication between phones/email and servers.

More than 3.5 billion people around the world use Facebook.

During the initial outages, according to our plan, company employees will be locked out of their offices and unable to use the Facebook-based security log in, making recovery more difficult, and if we do it, right impossible.

These facilities are designed with high levels of physical and system security in mind. They are hard to get into, and once you are inside, the hardware and routers are designed to be difficult to modify even when you have physical access to them. So it took extra time to activate the secure access protocols needed to get people onsite and able to work on the servers.

Since Facebook had done extensive work hardening their systems to prevent unauthorized access, that hardening will prevent fast recovery.

Server and data center redundancy will not help them because it does not help with a virus or software bug because it can replicate it, so redundancy cannot help here. This bug will also affect Instagram and Messenger, because of shared-code or a derivative of that code allowing it the bug to be replicated across all services, since they have not firewalled these services. It is part of a data harvesting algorithm by Facebook's design and is further proof their alleged intentions by recent whistleblowers.

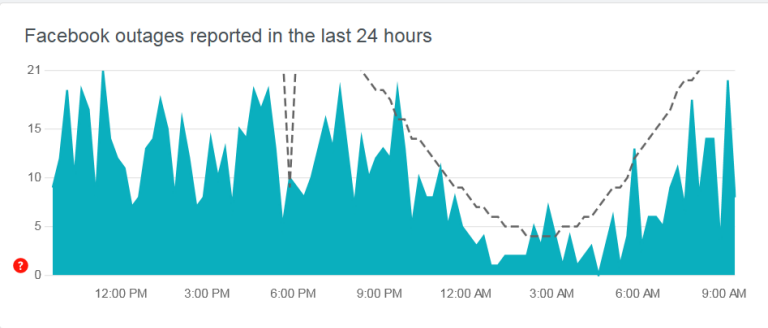
There was some discussion among the group about creating cooling-related failures in the buildings, but that was dismissed, as this would cause the service infrastructure to be powered down to prevent uncontrolled hardware failures. We really wanted to kill these machines

being used for evil purposes dead, permanently, including the over 100 PB of data stored in its data warehouse.

In general longer data center outages are becoming more common and more expensive. We aim to make this one the most expensive ever, via global termination.[48]

The Open Compute Project Foundation[49], an initiative that open sources and shares components of data-center design. This initiative standardizes data center design and makes it far easier for us to design and implement a hack.

We want this site to spike and then disappear.



https://downdetector.com/status/facebook/
https://metastatus.com/graph-api
https://metastatus.com/

[48] *https://www.datacenterfrontier.com/cloud/article/11427329/uptime-longer-data-center-outages-are-becoming-more-common*
[49] *https://www.opencompute.org/*

Facebook slowed everybody's Internet!
How did this then cause a slowdown of the internet? Billions of systems, including mobile devices running a Facebook-owned application in the background, were constantly requesting new "coordinates" for these sites. These requests are ordinarily cached in servers located at the edge, but when the BGP routes disappeared, so did those caches. Requests were routed upstream to large internet servers in core data centers.
The situation was compounded by a negative feedback loop, caused in part by application logic and in part by user behavior. Web applications will not accept a BGP routing error as an answer to a request and so they retry, often aggressively. Users and their mobile devices running these applications in the background also won't accept an error and will repeatedly reload the website or reboot the application. The result was an up to 40% increase in DNS request traffic, which slowed down other networks (and, therefore, increased latency and timeout requests for other web applications). The increased traffic also reportedly led to issues with some cellular networks, including users being unable to make voice-over-IP phone calls.
https://www.datacenterdynamics.com/en/opinions/too-big-to-fail-facebooks-global-outage/

The group was aware than taking down Facebook would disrupt a lot of businesses but believed that it was their fault for being lazy and cheap for not putting up their own websites and taking the easy and insecure route by using Facebook.

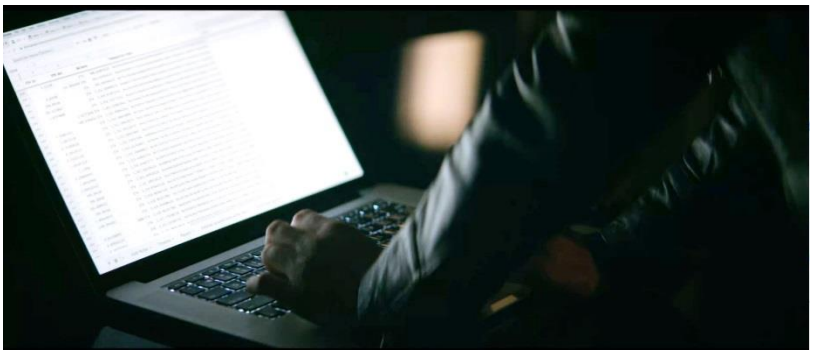
It might also put in danger some foreigners who stupidly were using an insecure system like Facebook, but they could always use something more secure like Signal instead.

The plan was starting to come together. Now all they had to do was build the malicious code.

To be continued…

Part Three: What is happening here?

http://www.the_insider_goes_deep/tales3.html



Even the smartest of search engines, like Google are thought by some to be only able to probe into around 16% of the content of the Dark Web. Others say about 96% of information is hidden underneath where the Deep Web is not indexed/crawled by any search engines including Google, Bing, and Yahoo. If this is true, it would mean that only about 4% is visible above the surface.

Tor itself has up scaled massively from being able to process around 50 GB per second, to more than 300 GB per second. Activity has increased by more than 300% in a few years, with around two million daily Tor browser users and with more than 30% of those users in North America. The Tor project and browser is thought to be actively used by around two million people around the world every day.

A King's College London study demonstrates the scope of this problem. According to these researchers, a series of scans of websites accessible through Tor (or "The Onion Router") confirmed that an identified 1,547 out of 2,723 live sites "were successfully classified" as containing "illicit content." The scan determined that the most common contents of these websites on Tor included "drugs, illicit finance, and pornography involving violence, children, and animals."

So what is in the Deep Web?

The Deep Web holds the content that is invisible to search engines. Here are a few examples of what is on the Deep Web:

The content of your personal email accounts

The content of your social media accounts

The content of your online banking accounts

Data that companies store on their private databases
Content contained within scientific and academic databases
Medical records
Legal documents

Viruses. Some websites could infect your devices with viruses, and there are many different types of viruses to watch out for. Remember to never download anything from websites CW or DW that you do not trust.

Hackers. You can find hacker forums on the dark web. You can hire computer hackers to do illegal activities. Not surprisingly, many of these people would be willing to hack your devices for money.

Webcam hijacking. A website on the Dark Web may try to get a remote administration tool, also known as a "RAT, onto your device. That can lead to someone hijacking your webcam, essentially letting them see what you are up to through your device's camera lens. It is a smart practice to cover your webcam with a built in cover or with a piece of paper or tape when not in use.

Meanwhile, some more sturm und drang[50] on the dread forum.

What would dread do?
by /u/KingBaldwin in /d/Dread
What would the other staff members do if Paris/HugBunter got arrested.
/u/Shakybeats M
1 points
Maybe we are all the same person.
/u/KingBaldwin
1 points
Multi-accounting isnt allowed ;)
/u/IMPERIYA-RELOADED
0 points
what if i have multiple personalities that are unaware of each other, do they not have a right to dread to?!
/u/KingBaldwin
1 points
Then yes, they have a right to make accounts.
/u/keydot77
1 points

[50] *German, usually translated as storm and stress.*

So they think...

/u/dank

1 points

/u/Reckless

1 points

Clearly they'd ignore the instructions on the Canary about waiting no more than 72 hours, because Hug's has been expired again for over a week.

/u/KingBaldwin

1 points

I dont even know why they have his canary up there, he is barely active but for a half-assed reason, "working on developments" last time he was working on them, dread was a shithole, he should honestly hand ownership to Paris.

/u/IMPERIYA-RELOADED

1 points

hug's version of 72 hours is alot different to ours it seems

/u/Reckless

1 points

That's my entire point, though. What's the point of using it as some form of safe guard if you're incapable of staying on top of it?

If you ask me, it being signed last time around doesn't even prove to me that he's alive. His Deadman URL also went down, we have no idea what level of information it contained. If his private key was in that dead drop anyone with access to it, which admittedly should probably only be Paris I would imagine, could have signed it.

He didn't make a post or anything explaining what happened or that he's alright. And to be fair, it's not mandatory for him to do so. It's just a stupid thing to have in place if you're not taking it seriously enough to find 60 seconds out of a 336 hour period to do it.

The shit exists so that if something did actually happen or if he did actually get compromised, appropriate measures could be taken to make sure shit keeps running and no further compromising would occur. It blows my mind how it's just shrugged off like "Oh, That Hug, He's such a silly boy! Im sure he's just drinking and relaxing"

There are those among us who would either abandon Dread completely, or change certain things up drastically if anyone at the top was to get compromised, but with the way these fail safes are handled nobody would know on time to do anything.

It's complacency, and there's no time for complacency in this business. Because look what happens when we have that.... All these exit scams, people losing money with plenty of prior warning that they are coming.

n0stis was surfing around The Hub one day and thinking about satisfying his 20 post minimum, so he posted the Demon Mouse story in three separate posts and added the offered poll.

The first round of reactions were thus:

Poll

Did you like this story and want to read more?

You suck newbie!

0 (0%)

Your story is shite!

0 (0%)

Wish I never read it!

1 (33.3%)

Liked it!

0 (0%)

Enjoyed it!

0 (0%)

May I have another please?

1 (33.3%)

My eyeballs are bleeding!

1 (33.3%)

Total Members Voted: 3

Author Topic: The Story of the Demon Mouse (Read 29 times)

n0stis

The Story of the Demon Mouse
It seems that my index finger carpel tunnel was acting up due to the extensive use of my DW research machine which was using a standard corded Microsoft mouse. My writing machine has had a Logitech roller ball (marble mouse) for many years due to this affliction from 30 plus years of index finger left clicking. So I ordered a new marble mouse (two day free shipping!) and installed it easily, no driver needed it used the 2006 MS driver and nothing newer came with it.
I then discovered this problem that every time I left clicked on something on a webpage it would revert to the previous page. Did it in Tor, in Firefox, and even in Pale Moon. But apparently nowhere else. So after rebooting the computer, no joy, and scratching my head a bit, I discovered a tiny button directly above the left and right click buttons which were present on my other marble mouse and certainly not authorized by me to do page forward and page back on the web. But did it anyway on its own as if demonically possessed.
So I carefully poked around the web a bit, very carefully clicking, and found out about some software Logitech wrote, or had written, to exert some control over these misbehaving demon buttons.
I made the mistake of clicking on the Chat button on the Logitech support page for assistance while looking for this miracle software and got taken down a deep dark rabbit hole of chat bot stupidity until I finally gave up on extracting anything intelligent from the bot.n0stis
Re: The Story of the Demon Mouse
« Reply #1
Anyway I eventually found the Options software and downloaded it and installed it only to discover it only works on Windows 10 and I certainly didn't want to go _there._ (See my previous book, The Cozening)
Continuing to carefully to sleuth around their web site, I found a version for Win7 buried there in a deep, dark hole of html code, downloaded and installed it only for it to present me with a window like it was looking for wireless devices, or cameras or anything other than a marble mouse. So foiled again. Rats!
So off I went to CNET downloads, an old reliable source of drivers and utility software, and found a piece of software called Mouse Manager from a company aptly named RealityRipple Software. It claimed that it could wrangle these rogue buttons and bring them under user control. n0stis
Re: The Story of the Demon Mouse
« Reply #2
Even though the software instructions said it could do the job for the fourth and fifth buttons, and I needed it to control the third and fourth buttons of this Satan incarnate mouse which I didn't ask for, I configured them to be disabled and that did the trick.
I am not sure who tested this marble mouse, but it was not me, or these useless buttons would have never seen the light of day, (cost reduction, Logitech send me a check please). Either that or I would have relented and

placed to the left and right of the marble, which is the only reasonable place for them to be.
Unfortunately , this software is a TSR. So it must stay resident in memory as a Tray Icon in Windows to continue to work. But I donated to the cause anyway because it worked for me.

Allegiance

- *Head Punch Monkey*
- *Global Moderator*
- *Legendary Contributor*
- *Posts: 3107*
- *Community Rating: +226/-77*
- *Drunk on power and high on Mod Crack*

Re: The Story of the Demon Mouse

« Reply #3

Obviously your whole setup is demonically possessed. Also, it's Windows, Satan's Operating System, so naturally these things will happen. At this point, your only option is to pour the blood of a dead crack whore over it, immolate it post haste with some thermide, cool the ashes with holy water while reciting Hail Mary, then deposit the ashes inside the carcass of the dead whore, sew her up with silver thread, and dump her in a lake.

Next, get a decent PC and never again access the Dark Net with anything other than TAILS or Whonix running over Qubes OS.

And remember... Satan is watching you!

"Allie often shares the mod crack with me " -T.P.V
"You don't have to be a weirdo to mod here but it helps " -Lucidity
"my wife is a non binary black transsexual amphibious all terrain attack trained doormat i beg your pardon very much still smells fishy, you better wash behind your ears and other places too"- Benihana
"Anyone who doesn't like pineapple on pizza is a cunt" - Lucidity

BenzoBore

- *Jr. Contributor*
- *Posts: 67*
- *Community Rating: +12/-0*
- *too based*

Re: The Story of the Demon Mouse

« Reply #4

hell of lot better than most introductory posts

it is in the darkness that you discern the most light
"never liked chasing the dragon as I'd usually end up chasing my own tail" - Beni

T.P.V.

- *Moderator*
- *Legendary Contributor*

- *Posts: 2269*
- *Community Rating: +129/-77*
- *If you're new welcome. If you're lost try Guides.*

Re: The Story of the Demon Mouse
« Reply #5
Quote from: T.P.V.
This is where you post newbies.
Also if you need to spam to get access to the other /threads the spamming can happen here.
I am not sure what you have posted here but even the mention of the word windows on here sends shivers down our collective spines.
Please read the HUB rules before posting. Encrypt PM's people.
benihana
Re: The Story of the Demon Mouse
« Reply #6
The marble is infected
Mandatory reading prior to communication attempts. Most unencrypted PMs are trashed.
sernace

- *Hero Contributor*
- *Posts: 774*
- *Community Rating: +85/-30*
- *Need a friend? get a dog*

Re: The Story of the Demon Mouse
« Reply #7
another basement dweller covered in cheeto dust. oh well

So back on The Hub n0stis responded to a forum post with an encrypted Private Message (PM):

Re: The Story of the Demon Mouse
« Reply #4 on: April 23, 2022, 10:54:50 AM »
Quote
hell of lot better than most introductory posts
it is in the darkness that you discern the most light

-----BEGIN PGP MESSAGE-----
Version: BCPG v1.63
Thanks for the only intelligent response post to my beginner messages.
I am a writer doing research for a historical novel about the Dark Web. I am not a journalist, but I am looking to have discussions with a number of people

on a number of topics on dread, The Hub, Raddle and maybe Envoy.

I think that you as a Hub subscriber would be a good choice for me if you are willing. I am not looking to expose anything other than get some ideas of who and why people are here and what they are doing. Am interested in legal activities only.

Email n0stis@mail2tor.com

-----END PGP MESSAGE-----

And now that n0stis can sit at the grownups table on the Hub anyway, he posted a message with a poll in the General Discussion forum or sub.

The Hub

I am a writer doing research for a historical novel about the Dark Web. I am not a journalist, but I am looking to have discussions with a number of people on a number of topics on dread, The Hub, Raddle and maybe Envoy.

I think that you as a Hub subscriber would be a good choice for me if you are willing. I am not looking to expose anything other than get some ideas of who and why people are here and what they are doing. Am interested in legal activities only.

I am looking to have discussions on these topics and others.

The Dark Web provides:

Freedom of or from politics?

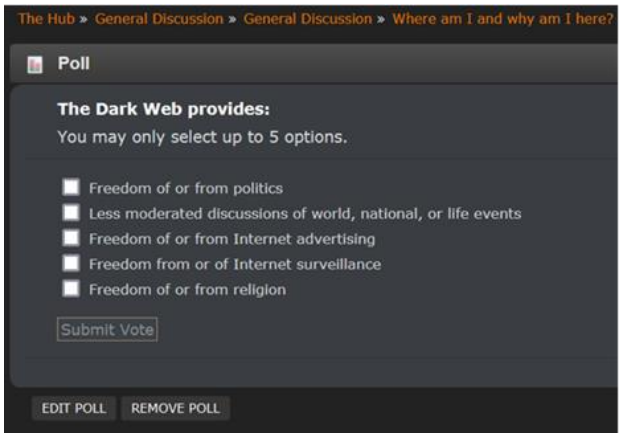
Less moderated discussions of world, national, or life events

Freedom of or from Internet advertising

Freedom from or of Internet surveillance

Freedom of or from religion

Email n0stis@mail2tor.com



Meanwhile, a first attempt at posting on dread resulted in a scolding from the mod.

/u/Solar M

Only posts relating to this site in this subdread allowed! Posts here are manually reviewed before public posting!

you will please note that most users understand that this type of post will make it easier to profile and is worthless to the user base. find appropriate subs for this and follow all site wide and sub specific rules.

/u/n0stis

Sorry, meant to post in CafeDread.

Is that OK?

So that begs the question of what is of value to the user base.

Submit a post to /d/cafedread 4,379 subscribers

Precious Metals

Post whatever you want, prepare to be shit on relentlessly if its gay.

Then came some reasonable, for the Dark Web anyway, discourse on Envoy.

- *Envoy »*
- *Cyber Insecurity »*
- *The Onion Router »*
- *The Garlic Network »*
- *I2P or Tor*

Author Topic: I2P or Tor (Read 1720 times)

keepinternetfree901

- *Newbie*
- *Posts: 12*
- *Penis Size +1/-0*
- *New Ambassador*

I2P or Tor

- *Quote*

Is it a better idea to use I2P or Tor.

n0stis

- *Newbie*
- *Posts: 1*
- *Penis Size +0/-0*
- *New Ambassador*

Re: I2P or Tor

« Reply #1

1300 geeks read this message and no one responded, so I thought I would newbie to newbie.

I use Tor but I believe that the answer to that question could likely fill a book. Quick take is that Tor is thought to be larger and more secure. But this is a simplistic view.

rickityslick

- *Newbie*
- *Posts: 33*
- *Penis Size +1/-0*
- *New Ambassador*

Re: I2P or Tor

« Reply #2

Quote from: n0stis

1300 geeks read this message and no one responded, so I thought I would newbie to newbie.

I use Tor but I believe that the answer to that question could likely fill a book. Quick take is that Tor is thought to be larger and more secure. But this is a simplistic view.

Apologies for having nothing of substance to contribute, but the view to response ratio of some threads/questions on here is pretty crazy. Participate people!

PGP - /index.php?topic=8.msg3151#msg3151

Loshobos

- *Newbie*
- *Posts: 2*
- *Penis Size +0/-0*
- *New Ambassador*

Re: I2P or Tor

« Reply #3

- *Quote*

I honestly have mixed luck setting it up and zero luck using virtual box/whonix. Tried some forums and manuals but some aspects are more complicated than TOR and that's the thing, if I can't use it properly and confidently am I safe.

rickityslick

- *Newbie*
- *Posts: 33*

- *Penis Size +1/-0*
- *New Ambassador*

Re: I2P or Tor

« Reply #4

- *Quote*

There was a Dread post describing how to use I2P with Tor which worked, but then it said something like "only use this to access AlphaBay's I2P address". I definitely need to education myself more too.

PGP - /index.php?topic=8.msg3151#msg3151

fuckifckedup

- *Newbie*
- *Posts: 21*
- *Penis Size +1/-1*
- *human. being. i didnt ask for this.*

Re: I2P or Tor

« Reply #5

- *Quote*

ive tried setting up a few of those networks like yggdrasil and i2p, or freenet. no luck with any of them to where i can use them like i do tor. exploring them is fun to me. freenet has a lot of cool sites up.

i was wanting to use i2p, just noticing tor.taxi is posting links. id thought it would be easier to access. i cant seem to get my plugins (foxyproxy) to work properly. we need a whole browser. that would make things easier.

interesting things are interesting.

Some less cordial but still interesting discourse.

Note: Thought you would like to see a sample DW forum advert.

- *Envoy »*
- *Dark Net Markets »*
- *OpSec »*
- *Education is a primary bottleneck.*

Author Topic: Education is a primary bottleneck. (Read 2129 times)

Pygmalion_copypasta

- *Newbie*
- *Posts: 39*
- *Penis Size +2/-0*
- *New Ambassador*

Education is a primary bottleneck.

Quote

Dear vendors,

One primary bottle neck of the growth of the DN is education.

Many people simply do not understand how to use PGP, purchase Monero, navigate to the DN, and order.

Therefore efforts should be made to bring more new people here.

The markets DDOSing each other are stupid because they deter potential new customers.

It's pretty inconvenient to try and purchase drugs in the middle of a bunch of imperialistic minded folks flaming each other with fire.

I invite these people to spend the valuable resources that they spend on destroying each other's infrastructure to build up educational websites instead, and get the word out more. That would not only bring more people here, it would allow us to conduct stable business and enjoy more money.

A smaller share of a big cake is better than a big share of a small cookie.

Vendors have the power to support markets who have good ethics and principles. Stop going to markets because of popularity.

Good vendors are the reason why these markets are popular. Instead, go to well coded markets that are run by mentally stable and peaceful people and help them grow.

This is a political issue.

Sincerely,Pygmalion

dude_user

- *Newbie*
- *Posts: 3*
- *Penis Size +0/-0*
- *New Ambassador*

Re: Education is a primary bottleneck.

« Reply #1

- *Quote*

Education and a lack of overall professionalism of vendor. thee markets are selling a lot of trash products with scammy vendo.rs. Even many of the decent one are a quasi scammy. It demoralizing after spending ur money to find out

the product doesn't help accomplish what is advertised

Witchman05

- *Administrator*
- *Sr. Member*
- *Posts: 323*
- *Penis Size +28/-0*
- *Patron Saint of Fools*

Re: Education is a primary bottleneck.

« Reply #2

- *Quote*

When education is not liberating, the dream of the oppressed is to become the oppressor. - Paulo Freire.

Archbishop. Revolutionary. Patron Saint of Fools. Admin. Author. Tinker. Tailor. Soldier. Spy. Magician. Your dream man, babydoll.
Viva la Envolution!
PGP key: /index.php?topic=8.msg12#msg12

allratsmustdie

- *Newbie*
- *Posts: 15*
- *Penis Size +1/-0*
- *New Ambassador*

Re: Education is a primary bottleneck.

« Reply #3

- *Quote*

I was always very impressed with the operational practices of White House Market. I was sad to see it go but I was always impressed by the forced use of Monero and PGP. I felt as though they were a pioneer in mandating the use of safest practices at the time.

I feel like Versus is the closest platform in comparison to White House at the moment... Thoughts?

Public PGP Key:
http://envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz2eg4skwmbyd.onion/index.php?topic=8.15

plkqcs

- *Verified Vendor*
- *Full Member*
- *Posts: 130*
- *Penis Size +56/-4*
- *New Ambassador*

Re: Education is a primary bottleneck.

« Reply #4

- *Quote*

Quote from: Witchman05 on April 17, 2022, 10:10:25 am

When education is not liberating, the dream of the oppressed is to become the oppressor. - Paulo Freire.

The vacuum of ignorance is filled with the fantastic - Erasmus

martinatchet

- *Newbie*
- *Posts: 1*
- *Penis Size +0/-0*
- *New Ambassador*

Re: Education is a primary bottleneck.

« Reply #5

- *Quote*

Quote from: allratsmustdie on April 21, 2022, 07:05:16 pm

I was always very impressed with the operational practices of White House Market. I was sad to see it go but I was always impressed by the forced use of Monero and PGP. I felt as though they were a pioneer in mandating the use of safest practices at the time.

I feel like Versus is the closest platform in comparison to White House at the moment... Thoughts?

I agree - trying to cater to everyone by allowing people to possibly compromise themselves is a very short-term focused decision. Yes you might lose users by requiring things like XMR, but you're guaranteeing some degree of safety for yourself and your users. I'd rather use a smaller, more secure market that functions well than a huge one that falters often.

allratsmustdie

- *Newbie*
- *Posts: 15*
- *Penis Size +1/-0*
- *New Ambassador*

Re: Education is a primary bottleneck.

« Reply #6

- *Quote*

Quote from: martinatchet on April 22, 2022, 03:37:22 am

Quote from: allratsmustdie on April 21, 2022, 07:05:16 pm

I was always very impressed with the operational practices of White House Market. I was sad to see it go but I was always impressed by the forced use of Monero and PGP. I felt as though they were a pioneer in mandating the use of safest practices at the time.

I feel like Versus is the closest platform in comparison to White House at the moment... Thoughts?

I agree - trying to cater to everyone by allowing people to possibly compromise themselves is a very short-term focused decision. Yes you might lose users by requiring things like XMR, but you're guaranteeing some degree of safety for yourself and your users. I'd rather use a smaller, more secure market that functions well than a huge one that falters often.

I'm curious to see if another market rises that advocates for security/safety such as WHM. The admin of WHM was also a pleasure to work with. Mr. White (I think was his tagname on Dread), the retired admin of WHM, was always very friendly and helpful in his discussions with new users on Dread. Hopefully he is sitting on on a beach with a drink in hand enjoying his/her retirement.

Public PGP Key:
http://envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz2eg4skwmbyd.onion/index.php?topic=8.15

YosemiteGhostWrite

- *Newbie*
- *Posts: 36*
- *Penis Size +57/-0*
- *CEO of Sex*

Re: Education is a primary bottleneck.

« Reply #7

- *Quote*

"Dicks in my mouth" - Witchman05

"Imagine to imagine" - YGW

Witchman05

- *Administrator*
- *Sr. Member*
- *Posts: 323*
- *Penis Size +28/-0*
- *Patron Saint of Fools*

Re: Education is a primary bottleneck.

« Reply #8

- *Quote*

Quote from: YosemiteGhostWrite on April 25, 2022, 10:45:29 pm

"Dicks in my mouth" - Witchman05

"I once sent nudes to DarkDotFail." - YosemiteGhostWrite, 2021.

Archbishop. Revolutionary. Patron Saint of Fools. Admin. Author. Tinker. Tailor. Soldier. Spy. Magician. Your dream man, babydoll.
Viva la Envolution!
PGP key: /index.php?topic=8.msg12#msg12

QuickieFlippie

- *Jr. Member*
- *Posts: 53*
- *Penis Size +7/-0*
- *Pro Reviewer on Dread, not here...YET!*

Re: Education is a primary bottleneck.

« Reply #9

- *Quote*

Balls in your jaws

"Do your job"

Rorschach_9000

- *Global Moderator*
- *Full Member*
- *Posts: 155*
- *Penis Size +16/-1*
- *RIP_Meth_9000*

Re: Education is a primary bottleneck.

« Reply #10

- *Quote*

The problem is the Bible, it sucks!!!!

Definitely does not go far enough or give noobs a bigger field to choose from.

Everyone who swears by Tails is definitely putting yourself at risk. It does nothing to protect your real IP address.

Don't believe me, go ask William Gibson of Versus what os he uses & why.

People just think I'm a ruthless ass hole when it comes to noobs, in actuality I am treating them as they should be treated.

They fucking need tough love!!!!

This shit is no game, it's a real as it gets & our adversary is getting stronger day by day!!!

I blame the mod's in the DNM sub on Dread for part of this issue!!!!

They fucking coddle these noods too much!!!!

They need in your face advice that clearly states the right way to do this & they definitely need to know the most severe way this can end!!!!

To quote one of my all time favorite movies Office Space!!!!

A Federal POUND You In The ASS Prison!!!!

It's definitely time I give Tyrone his own thread here on Envoy telling noobs that he & his 13 inch BBC is waiting on that sweet noob ass!!!!
Female Body Inspector
You can find my PGP key here...
http://envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz2eg4skwmbyd.onion/index.php?topic=8.15

Let us take a break here and ponder what was said by someone who has been promoted to n0stis as a premier DW'er, /u/9k and his multiple variations of that name.

He said that Tails does not protect the identity of your IP. Since most common Linux DW variants, Whonix, Qubes, Tails, etc. are based on Debian that does not sound good to n0stis for general purpose DW OpSec.

ToGoPacks

- *Newbie*
- *Posts: 13*
- *Penis Size +1/-0*
- *New Ambassador*

Re: Education is a primary bottleneck.

« Reply #11

- *Quote*

Quote from: allratsmustdie

Quote from: martinatchet

I was always very impressed with the operational practices of White House Market. I was sad to see it go but I was always impressed by the forced use of Monero and PGP. I felt as though they were a pioneer in mandating the use of safest practices at the time.

I feel like Versus is the closest platform in comparison to White House at the moment... Thoughts?

I agree - trying to cater to everyone by allowing people to possibly compromise themselves is a very short-term focused decision. Yes you might lose users by requiring things like XMR, but you're guaranteeing some degree of safety for yourself and your users. I'd rather use a smaller, more secure market that functions well than a huge one that falters often.

I'm curious to see if another market rises that advocates for security/safety such as WHM. The admin of WHM was also a pleasure to work with. Mr. White (I think was his tagname on Dread), the retired admin of WHM, was always very friendly and helpful in his discussions with new users on Dread. Hopefully he is sitting on on a beach with a drink in hand enjoying his/her retirement.

You should check out the new Alphabay then. Their forums are very informative also.

Note: A DW search of Versus reveals a dead link as below, and so it goes on the DW.

http://3bbad7fauom4d6sgppalyqddsqbf5u5p56b5k5uk2zxsy3d6ey2jobad.onion/v?q=mirror.77eofv5tztxrlwek24ey6aiozqu3fn4opqus7qwg24bahyfxrjmttayd.onion

Versus dark marketplace
Versus Market is a new security driven marketplace that quickly growing. It features one of the best UI of any darknet market with very simple to use search options. Versus Market is a very good alternative to other top darknet markets.
3bbad7fauom4d6sgppalyqddsqbf5u5p56b5k5uk2zxsy3d6ey2jobad.onion — 2 weeks, 4 days ago —

This site links to an onion search that comes up empty.

And of course, some more wailing and gnashing of teeth about dread, the site they love to hate. Especially on other DW sites like Hub and Envoy.

- *Envoy »*
- *General »*
- *General Discussion »*
- *Dread FUCKING Sucks / Too Damn Slow!!!!*

Author Topic: Dread FUCKING Sucks / Too Damn Slow!!!! (Read 75 times)

Rorschach_9000

- *Global Moderator*
- *Full Member*
- *Posts: 156*
- *Penis Size +16/-1*
- *RIP_Meth_9000*

Dread FUCKING Sucks / Too Damn Slow!!!!

- *Quote*

Really, what the fuck?
Shit won't fucking load, can't see my replies!!!
When will people get tired of that shit show?
Female Body Inspector
You can find my PGP key here...
http://envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz2eg4skwmbyd.onion/index.php?topic=8.15
rickityslick

- *Newbie*

- *Posts: 33*
- *Penis Size +1/-0*
- *New Ambassador*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #1

- *Quote*

Incredibly frustrating...and literally happening at this moment after getting new identity which of course signs you out of everything. Get the encrypted chat shit goin' that'd be great. Peace.

PGP - /index.php?topic=8.msg3151#msg3151

Pygmalion

- *Verified Vendor*
- *Jr. Member*
- *Posts: 53*
- *Penis Size +56/-0*
- *Drugs and Chemicals Vendor*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #2

- *Quote*

I bet the main reason why Dread is so slow is not DDoS but the sheer size of their software and userbase.

MDMA, Cocaine, DMT, LSD, Ketamine, Speed Sulfate, Speed Paste, 2C-B, Magic Mushrooms BUY BUY BUY

Rorschach_9000

- *Global Moderator*
- *Full Member*
- *Posts: 156*
- *Penis Size +16/-1*
- *RIP_Meth_9000*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #3

- *Quote*

I can't even get a new post window to fucking open!!!!

FUCK DREAD!!!!

Female Body Inspector

You can find my PGP key here...
http://envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz2eg4skwmbyd.onion/index.php?topic=8.15

Pygmalion

- *Verified Vendor*

- *Jr. Member*
- *Posts: 53*
- *Penis Size +56/-0*
- *Drugs and Chemicals Vendor*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #4

- *Quote*

FUCK DREAD would be a great black techno song title.

MDMA, Cocaine, DMT, LSD, Ketamine, Speed Sulfate, Speed Paste, 2C-B, Magic Mushrooms BUY BUY BUY

Rorschach_9000

- *Global Moderator*
- *Full Member*
- *Posts: 156*
- *Penis Size +16/-1*
- *RIP_Meth_9000*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #5

- *Quote*

I am so frustrated at it right now!!!!

Female Body Inspector
You can find my PGP key here...
http://envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz2eg4skwmbyd.onion/index.php?topic=8.15

Pygmalion

- *Verified Vendor*
- *Jr. Member*
- *Posts: 53*
- *Penis Size +56/-0*
- *Drugs and Chemicals Vendor*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #6

- *Quote*

FUCK

MDMA, Cocaine, DMT, LSD, Ketamine, Speed Sulfate, Speed Paste, 2C-B, Magic Mushrooms BUY BUY BUY ToGoPacks

Newbie

- *Posts: 13*
- *Penis Size +1/-0*
- *New Ambassador*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #7

- *Quote*

The only thing I have learned from dread is that the most pro active vendors are scammers. Straight to business vendors move in silence and can be found on markets, not forums.

Witchman05

- *Administrator*
- *Sr. Member*
- *Posts: 326*
- *Penis Size +28/-0*
- *Patron Saint of Fools*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #8

- *Quote*

Quote from: Rorschach_9000

Dread FUCKING Sucks / Too Damn Slow!!!!

Orlok the Assassin be like.
Archbishop. Revolutionary. Patron Saint of Fools. Admin. Author. Tinker. Tailor. Soldier. Spy. Magician. Your dream man, babydoll.
Viva la Envolution!
PGP key: /index.php?topic=8.msg12#msg12

Rorschach_9000

- *Global Moderator*
- *Full Member*
- *Posts: 156*
- *Penis Size +16/-1*
- *RIP_Meth_9000*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #9

- *Quote*

I'm freaking hardwired direct into a very fast connection & its still hard as hell to open!!!!!

Female Body Inspector
You can find my PGP key here...
http://envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz2eg4skwmbyd.onion/index.php?topic=8.15

allratsmustdie

- *Newbie*
- *Posts: 20*
- *Penis Size +1/-0*

- *New Ambassador*

Re: Dread FUCKING Sucks / Too Damn Slow!!!!

« Reply #11

- *Quote*

Quote from: rickityslick

Quote from: ToGoPacks

The only thing I have learned from dread is that the most pro active vendors are scammers. Straight to business vendors move in silence and can be found on markets, not forums.

Interesting thought that I never considered, but I think you're definitely right. Some of the vendors I've had the worst experiences with I see on there often, blasting their own praise or advertising.

Some vendors/businesses are better at marketing than they are on focusing on day to day operations of their businesses.

I have also discovered some of my best vendors through forums, Dread included, thanks to the advice of mods and OP's (Yourself included 9000...)

After seeing this the same day, n0stis logged into dread and saw this tidbit.

ck it Onion Search Engines I'll Have What He's Having Honors

DDOS and DNM's

by /u/emptyzin74 in /d/CafeDread

Hello there, i always had this question, but never got a good response..

Why and who keeps ddosing dnm's, this always been a thing, but who would waste their time and money making large attacks on markets, whats the point of this?

Regards,

/u/SplinterCell

Blackmail.

Hackers regularly go after websites and services such as gambling websites or markets. Here is an example of the Silk Road admin paying a hacker $15,000 to prevent an attack because it was just cheaper to do so than have their market down.

"On at least two separate occasions, Silk Road operators paid malicious attackers ransoms in exchange for keeping the site up and secure. "

https://www.computerworld.com/article/2877052/silk-road-paid-thousands-in-shake-downs-from-malicious-hackers.html

It happens to legitment businesses too:

https://www.channelweb.co.uk/news/2431257/uk-e-tailers-hit-by-ddos-barrage

It is easier to go after businesses that cannot go to the police.

Sometimes paranoia rules the day on the DW, in addition to the traditional poor grammar and spelling common in certain circles among those who believe this attention to detail to be only for the elites. To some such stupidity apparently is now being viewed as a superpower.

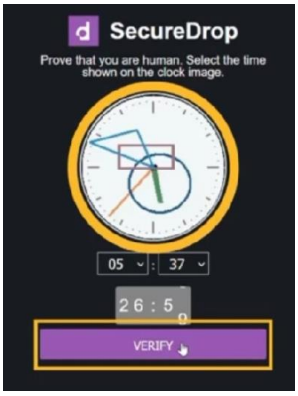
Something interesting:

Why is US State Depatment using Dread's captcha?

by /u/Blanksee in /d/CafeDread

It's literally the same ...

PrtScr image from the departments onion service 'SecureDrop' :



http://uoxqi4lrfqztugili7zzgygibs4xstehf-5hohtkpyqcoyryweypzkwid.onion/?img=271651932610.jpg

Why is that?

/u/Paris A 2 points

They are using /d/endgame which is an open to all. Including the Feds.

/u/marktwain0000 2 points

The fucking feds using your own old captcha. I would be proud haha.

/u/Blanksee 1 points

That's pretty newsworthy itself

/u/BlickyBandit75 1 points

Pretty sure the US government created tor to communicate anonymously but had to open it up to everydody to blend in. there is some sort of link there

/u/burndownmf 0 points

What could possibly be the reason why uncountable onions use that or a similar looking captcha? Might it be open source and published here on Dread? Oh no, your stupid conspiracy theory just faded in the wind.

WIP: Recommended List of E-Mail providers

by /u/[deleted] Vendor Opsec • in /d/OpSec
Dear Community,
Let's build a list of recommended anonymous email providers.
They need to meet the following criteria:
1. Anonymous registration possible as a feature, not a hack.
2. Tor friendly
3. Fully functional connectivity with other providers
4. No javascript required
My personal picks:
Public:
protonmail.com:
Pro:
Under Swiss law.
Onion support
PGP support
Encrypted mailbox
Con:
Under Swiss law.
Requires some tech savvy to really use with full opsec.
Invite only:
infantile.us
Infantile is only for the best and brightest users of the DN. If you get one, it's a stamp of approval of your character and service.
Link:
http://juvenilezskkwc2gu7j5c4akppjnr3kzlgljjeodd5psn6fwcnloplid.onion/
Run by /u/Kaizushi. 100% pirate. 100% awesome.
riseup.net
Pro:
Onion support
Can request tor bridges (only other provider is gmail)
US law (5th ammendment)
Really easy to use with full opsec.
Con:
US law
Please state your recommendations below.
Sincerely,
Pygmalion

/u/astrix

4 points

darknet mail exchange: dnmx.org

http://hxuzjtocnzvv5g2rtg2bhwkcbupmk7rclb6lly3fo4tvqkk5oyrv3nid.onion

/u/gencoch

1 points

Just my experience:

I have tried for two days to sign up for a dnmx account. No matter how many times I try I keep getting a CAPTCHA invalid message. I know damn well I ain't messing up the CAPTCHA.

No matter whether it's been DNMX, or Elude, or SquirrelMail - my experience with all these darknet email services is that they seem to suck when it comes to actual usability. Frustrating as fuck...

/u/astrix

2 points

FYI: The captcha for creating a dnmx account is case sensitive

/u/gencoch

1 points

I owe you bro!

/u/qualifiedrc2

1 points

same ive been getting the captcha 100% CORRECT and still it wont work shit is soo frustrating. Eludes clock captcha is the worst one it would NOT let me through.

/u/We_Are_9000 Paranoia Level

3 points

Gmail

Yahoo Mail

Hot Mail

/u/FUDPolice

2 points

Miss the old yahoo / hotmail days. Reset password by answering favourite movie.

Ok, what movies do they like on social media. Starwars? Bingo. Next minute icloud backups remotely downloaded and devices wiped.

Easy as =)

/u/IamLegion

1 points

I remember yahoo/msn messenger would alt-tab you out of a game running

on full screen if someone buzzed you so everybody kept spamming the buzz to piss people off

/u/HeadJanitor Moderator

3 points

Mail2Tor

https://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion.ws/

/u/LydiaRQ

2 points

"In their ToS they say they collaborate with LE, but still worth a mention simply because they are awesome folks."

I agree. Rise Up is LE-level phishing but no biggie. I've met some awesome folks in prison as well. They will feed and take care of you there so it's okay because what's important is to be around awesome folks.

/u/Pygmalion Vendor Opsec

1 points

Dread is also a federal honey pot. Everything is a honey pot.

Your opsec assumes that, right?

/u/LydiaRQ

1 points

Indeed. Don't know how much LE activity there is here, yet one opsec necesity is always to use PGP. Many do not for some reason be it lazy or otherwise.

/u/pharoah P

1 points

Cheers!

/u/OhLongJohnson

1 points

And what about elude.in?

/u/Pygmalion Vendor Opsec

1 points

Lots of connectivity issues.

/u/OhLongJohnson

1 points

Yeah, it is more offline than working, but in security how it is?

/u/Pygmalion Vendor Opsec

2 points

I don't know. Any claims about security are just marketing lies.

They were never hacked to my knowledge, so there is that.

/u/nagoya
1 points
Invite only: cock.li
/u/Sciencier
1 points
Can somebody send me an invite link?
/u/HeadJanitor Moderator
1 points
(private: spelling error)
/u/HeadJanitor Moderator
1 points
Cock.li
Website:
rurcblzhmdk22kttfkel2zduhyu3r6to7knyc7wiorzrx5gw4c3lftad.onion
Mail: xdkriz6cn2avvcr2vks5lvvtmfojz2ohjzj4fhyuka55mvljeso2ztqd.onion
/u/HeadJanitor Moderator
1 points
https://www.torbox.ch/
TorBox supports OBFS4, Meek-Azure and Snowflake bridges, which help to overcome censorship (with an easy to use interface).
/u/HeadJanitor Moderator
1 points
SecretMail
http://2nxpboa3ya52j5au4gxwkdt4nxoh5g4y4f3tuqedlza46y35jmv6doid.onion/
/u/Eludedowntime
1 points
Tried Sector, it did not receive a single email.
/u/socat2me
1 points
Same here, never received any mail.
/u/gencoch
1 points
SquirrelMail just allowed me to create two email accounts with the very same user name.
I only tried a second time because I was curious to see if the first effort took. After supposedly successfully creating the account, abd receiving a message I could log in, I tried to do so but could not.

So I decided to try and once again register an account. I used the same exact user name and changed the password. I received the notification that I had successfully registered, and could try to log in. I tried but I could not.

That's gonna be the extent of my effort with SquirrelMail. That the same user name could be registered twice is sufficiently concerning to me to consider that email service to risky.

/u/HeadJanitor Moderator

1 points

hobe onion mail

http://ovhcd6qhuz22bid42pw7unwfqf7i55rghb5x62q4kxchjnk2gz2ot6id.onion/register.html

/u/HeadJanitor Moderator

1 points

hidden mail onion server

http://5nm4mdhzyfbif6i5qv3kh4i7j2trlbuvujsencsqn55opaa3d6qhfcqd.onion/register.html

/u/HeadJanitor Moderator

1 points

dozaru onion mail server

http://eot3almpracnkz7gz3r5yr3qaymngqsrmvbica2shw5zuc52az2gxoqd.onion/info.html

/u/kaizushi

1 points

Infantile.us as a clearweb site is just an introductory point to Tor in general. The hidden service that would be relevant in your post here /u/Pygmalion is...

http://juvenilezskkwc2gu7j5c4akppjnr3kzlgljjeodd5psn6fwcnloplid.onion/

It has my contact details at the bottom of the page. Also I don't just accept anyone as my customer and intend only to sell services to the darkweb's best and brightest. You need to be someone with a history of activity, good character, and such to get an account and your listing here should point that out.

/u/Foo9eeng

1 points

your service is not an email provider

hence, why you post?

/u/Pygmalion Vendor Opsec

1 points

Corrected, thank you. Please let me know if you want me to add anything.

/u/kilo

1 points

cock.li will forever be best, for providing emails such as @420blaze.it and @cocaine.ninja. They also provide some that are highly offensive, which I don't agree with, such as @nuke.africa and @nigge.rs, but I can live with those ones existing if it means I get to keep my @420blaze.it and @cocaine.ninja. Some others that come to mind are @cumallover.me emails.

They went invite-only recently so now it's rare for newcomers to get themselves one.

/u/floatingzero

1 points

That's free speech for you: you take the rough with the smooth. You have the right attitude towards it.

/u/floatingzero

1 points

>riseup.net

>In their ToS they say they collaborate with LE, but still worth a mention simply because they are awesome folks.

Kek. Not only are those Marxists not "awesome folks" but the fact that they cooperate with LE is fucking hilarious. Nice autonomous anarchist community you've got there, lads. I'm glad I let my account expire.

Anyway, what's wrong with the classic clearnet providers like Proton and Tutanota? I mean, I'm sure there's something wrong with them - they're too big not to have been tapped up - but IDK what it is specifically.

/u/fanin12of7

1 points

I personally use tutanota and onionmail as my work emails

onionmail - http://pflujznptk5lmuf6xwadfqy6nffykdvahfbljh7liljailjbxrgvhfid.onion

hope this helped ^^12of7

/u/DRUGZRUS P

1 points

I haven't seen ProtonMail listed. Anything against them?

Clean isolated OS or VM > VPN > TOR Browser > https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/

/u/ioioio

1 points

some of: JS is forced, JS is not OpSec friendly.

some say they proton co-operate with others more easy thank they thinks

/u/DRUGZRUS P

1 points

Thanks. Yea I know about the JS part. Using Qubes and Whonix with disposable VM or hardened dedicated VM that only accesses ProtonMail seems good. I like that their systems have gone through several third party audits and passed.

Only cooperation with LE that I recall reading about was for a terrorist suspect and even with that the only thing they were able to provide was the IP address. So if accessing over VPN and TOR seems sufficient for good OPSEC.

/u/ioioio

1 points

you may be right and thats good idea hardended system

i was told other things by trusted sources

i don't say yes or no on this

/u/DRUGZRUS P

1 points

Yea I'm definitely not claiming to be an expert on that but it seems reasonably secure for that specific use case

/u/ioioio

1 points

[removed]

/u/Pygmalion Vendor Opsec

1 points

I'll put 'em on there with the stuff you need to know.

/u/DRUGZRUS P

1 points

Cool thanks!

/u/vekocy

1 points

DNMX.org - No CSS, Plain jane ugly web based email.

Insider Story Three </html>

- ***Third Goal: We will modify the RealOS WinFS file system to work on top of the Didgets operating system database to interoperate with the proposed P2P (Peer-to-Peer) Mixnet networks.***

Note: you may recall from my previous book "The Cozening" that one of the main technical features of the RealOS WinFS was adapting a SQL database engine as a component of the NTFS file system and create a much more sophisticated set of data types and objects that could be stored as files and also allow for very advanced views of all of the types of data a user might want to store.

For the third goal, it had been jointly decided that the primary software developers will be /u/wintermute, /u/syntax. The new group would not use a blockchain database for Web 4 since they do not lend themselves to data queries very well, and the security provisions were still very unclear at this time. They would instead modify the RealOS WinFS client software to sit or layer, on top of Digits rather than NTFS and provide these queries, decentralized on each device in a peer-to-peer decentralized Mixnet network.

It became clear that we would need to add database expert Andy Lawrence to the team to adapt his beta Didgets database to our new goals. Andy explained his creation in this way:

"Didgets (short for data widgets) are intelligent data objects that can efficiently manage large amounts of unstructured or structured data. It is a file system (NTFS, APFS, UFS, ext4) replacement." He went on to say, "I did have a distributed data store in mind as I designed Didgets originally. I envisioned the whole Didgets ecosystem as a global, distributed system called 'The Didget Realm'. When this becomes a reality, there will be millions (or billions) of individual 'Didget Nodes' in this system. Each node consists of a remote interface, the manager software, and a logical container (a pod). A node can effectively manage millions of different kinds of Didgets in a fast, efficient manner. Each node is a member of a 'domain' that consists of one or more nodes. All nodes within the domain can share, exchange, synchronize, and protect data between them.

He continued: "So an individual or company would have a set of nodes within a domain that effectively manages all their data across many different physical devices connected via the Internet. Nodes

from different devices share information, but in a restricted manner. In order to accomplish this, data must be easily distinguished between data that was created within the domain (private or semi-private data) and data that is just a copy of data created somewhere else (public data)."

"Nothing other than pure and unbridled greed induced the idea of harvesting the data of all the people in the world for massive corporate profits, and government surveillance. I think the reason why the Internet has gravitated to the current centralized model where a few mega-players control vast amounts of data, is because good systems that effectively manage data in a distributed model have been lacking. Didgets was designed to rectify this."

Each Didget in the system is assigned a 64-bit number, as an identifier at creation and it never changes. There are 4 different 'classes' of Didgets (Public, Private, Semi-Private, and System). The top 2 bits in the ID indicate the class. This means that each class has 2 ^ 62 (or 4 million trillion) possible values. Public Didgets are ones that are published for general distribution and can be copied anywhere within the Realm. Private Didgets are specifically created by the user and can be copied anywhere within the user's domain. Semi-Private Didgets were also created for the user, but were created on their behalf by some program (e.g. Config files, user preferences, browser bookmarks, etc.). System Didgets are used to store internal data structures and have no meaning outside of a particular node (e.g. used/free bitmaps, tags, internal tables, etc.).

So if you have a million photos and 60% of them were created by you (i.e. you took the picture with your phone or digital camera) and the other 40% you downloaded from various places on the Internet, then you can easily distinguish between the two sets. If you edit a public photo, it keeps the original (public Didgets are immutable) and it makes a private photo from your changes.

Since public Didgets are immutable, all copies of the Didget are the same. If Microsoft, for example, publishes a public Didget (e.g. a Windows 11 network driver version 2.30) that is assigned the ID of 1234, then all copies of Didget 1234 around the world are the exact same. If an updated driver is later released, (e.g. version 2.31), it will be given an entirely different ID (e.g. 2345). Updating software therefore never patches the old version it replaces it. The entire operating system (if it were distributed as Didgets) would be described in 'Set Didget' that contains the IDs of every component. Theoretically, it should be possible to have 100 different versions of an operating system installed at the same time within a single Pod. You could just pick which one you wanted to boot at system startup. It would be very similar to the way

Git (source control software) behaves. Every committed change has its own hash and you can roll back to any point in the development process.

If your copy of a public Didget was damaged or accidentally deleted, you should be able to ask any number of other nodes in the Realm for a copy. If the Didget was popular, it should only take a few queries to find one from a nearby node. The Realm would enable the creation of a global content distribution system. A content owner (musician, author, developer, or movie producer) could release a public Didget of their creation. Once released, the Didget would be able to be copied anywhere within the Realm. The system allows Didgets to be 'locked' meaning that a key is needed to access the content. The key would be a private Didget. So the Realm would be like a giant 'Digital Vending Machine' where content is available for instant access. All you have to do is put your quarter (or dollar, or bitcoin) in the machine to unlock the content you want. Since the key is private, it can be copied to any other node within your domain. If you unlock a movie, you can access it across all your devices.

The idea is to have a system of millions of nodes, each one containing millions of Didgets, that can interact with each other in a peer-to-peer network. Didgets can be discovered by their IDs or by searching for Didgets with certain tags. Once discovered, they can be copied from one node to another easily. No central authority like Facebook or Google is required, nor will it be allowed.

Andy continued, so you might be thinking about asking about privacy, DRM, IP rights, malware, across a P2P and unlike Napster or BearShare for example.

Each Didget Node has full control over what Didgets are accessible. Any Didget can be locked and can only be accessed using a key. This mechanism is how a DRM system would be used. The content owner would lock their content and provide the key when payment (or other conditions) are met. In order to publish a Didget as a public item, the owner would have to prove their rights to do so. Malware could still take the form of a Didget, but once discovered it could easily be cleaned off the whole Realm since its ID would be known and can be dealt with.

The Didgets platform is built using three basic principles.

1. Break down data into simple, compartmentalized components that can be stored, combined, and manipulated independently using intelligent data objects called Didgets. Each type of Didget shares common attributes, but also has unique capabilities. A Didget can be useful on its own, but each one is also built to be easily combined with other Didgets to form more complex structures like relational tables or file hierarchies.
2. Attach meta-data tags to these Didgets so that groups of them can be easily found and organized even when there are large numbers of them. It is much more than just 'finding a needle in a large haystack'. It is finding a million specific needles spread across a billion haystacks in record time.
3. Organize the data and use efficient algorithms so that large amounts of data can be processed in parallel. Use the power of modern, multi-core CPUs to get results in a fraction of the time.

Back to the task of destroying Facebook.
Or could be design and implement an EMP attack?

To be continued…

Interlude

You may ask what this writers overall impression of the DW forums are at this point and you would be right to ask.

The DW inhabitants are in my experience very unlike the media portrayals of assassins, drug fiends, and pedophiles, but yet are a mostly revolting, disgusting, and disquieting collection of human beings just the same. This writer will concede however that he did not go looking to find this media narrative, nor participate in what might be viewed as solely drug markets or seek out criminal activities with no mixed legal/illegal value.

You will see this all play out in the Tales from the Dark Web chapters. This is however, fiction, and composites of actual characters were constructed and are this writer's sole responsibility.

While it is possible to have rational and intelligent discussions outside of the forums themselves, the discourse within the forums are childish, grammatically error prone, (despite active spell checking, indicating a degree of laziness) defensive, with the mods going out of their way to discourage participation or rational Q and A conversations. Much of this can be attributed to the distain of these elder spokesmen (many teenagers) for noobs who did not have to come up the hard way to get to this point, as they did. Then there are the sycophants, (also mostly teenagers) trying to get into the good graces of the elders by significant ass kissing or brown nosing.

This writer found those persons he corresponded with, composited within these pages, to be at times rational, intelligent, well read, fully aware of the world around them, and very capable of articulating their ideas as well as relevant literacy references, albeit only to obscure and bizarre literature.

After all, you need to be at least half smart, and have your whit's somewhat about you, drug addled, criminally intentioned, or not to survive here. It takes persistence as well to navigate this space with the CAPTCHA's, message and file encrypted OpSec, as well as all of the DW technologies and lingo.

As you have read in these pages previously, and will continue to see subsequently, when holes are shot into arguments and opinions (the few reasonable and rational ones made) they disengage or resort to name calling or other insults.

It does not seem possible to have a rational and reasonably intelligent discourse with this demographic, however generalizing and broad that may seem to the reader.

After a lifetime of being online, n0stis was sick of the DW after several months. He argued with these idiots, took a lot of verbal abuse in an effort to tell a story. The reader can decide if it is a good one and worth the effort.

These experiences in the DW certainly leave open the question of what could be if that passion for privacy, freedom, and technological talent could be redirected to be of more productive use to a larger society and perhaps to the entire world.

Because of the COVID pandemic, which already has or will eventually change everyone and everything, human talent is no longer sequestered to geographical areas (i.e. Silicon Valley, Austin, Madison, New York, Detroit) or even within artificially created office spaces. Talent can be everywhere and anywhere. This talent is being to a small extent, and can be further harnessed with the help of a private decentralized Internet communications vehicle and smart computers (end points) that are not part of a for profit and mass surveillance-intentional network.

The Insider stores herein and its companion book, provide an accounting of what that could look like.

We have the ability to progress as a civilization if we choose not to be a solely transactional and coin operated, carbon based bipedal species.

Ask yourself this question. When you stop at a gas station to make a purchase, why does your identity need to be part of that transaction? Why is not verification of funds sufficient?

Common Knowledge: The Dark Web is full of random gibberish written by random and disturbed people. (Or perhaps they are AI bots with gibberish generating keyboards)

Spend some time on the Dark Web and see if this is true for you or not.

The guide I have written for that task is the Encyclopedia Cyberspacia companion book.

Part Four: Does anybody know what time it is?

http://www.the_insider_goes_deep/tales4.html

A timeline for the history and rise of the Dark Web

Tor is based on the principle of 'onion routing' which was developed by a team led by Paul Syverson, and included Michael G. Reed and David Goldschlag at the United States Naval Research Laboratory in the 1990's.

This software was based on the work of inventor and cryptographer Dr. David Chaum in the early 1980s who foresaw and upcoming privacy problem with the Internet. He wanted to eliminate the possibility of future mass surveillance and focused specifically on email. He used encryption to not only protect the contents of the message but also the metadata about source and destination using what is called a Chaum Mix.

The alpha version of Tor, named 'The Onion Routing Project' or simply TOR Project, was developed by Roger Dingledine and Nick Mathewson. It was launched on September 20, 2002. Further development was carried under the financial roof of the Electronic Frontier Foundation (EFF).

With the release of private browsing networks like Tor, collections of Dark Websites and a subsequent community of followers began to emerge in full force. Wikipedia

Though many Dark Websites were formed to help those living under oppressive governments push back against censorship, the temptation of having a corner of the Internet where you could browse anonymously fueled a rise in the number of Dark Websites that hosted illegal content.

Then in 2009 we saw the release of Bitcoin. Before cryptocurrency was invented, illegal transactions on the Dark Web were hard to complete, as customers could potentially be located thousands of miles away and neither party wanted to risk using credit cards or PayPal for transactions because they leave paper trails.

In 2010: The Dark Web saw a rise in illegal transactions but yet served a benevolent purpose in late 2010 during the Arab Spring. Tor browser now more accessible to users and activists, needed it during this time. Tor not only protected people's identities online, but also allowed them to access critical resources, social media, and blocked websites.

In 2011, a Gawker-affiliated blog published an exposé on the Silk Road, marketplace that made buying and selling illegal drugs as easy as buying used electronics. This exposé drove more traffic straight to the Silk Road boosting its sales.

In 2013, the FBI successfully completed a sting and shut down the Silk Road. This was a historic sting, since the Silk Road drew close to a million users at one point.

Also in 2013 with the historic: Snowden Whistleblowing, demand for tools to protect against mass surveillance became mainstream. Tor was instrumental in aiding Snowden's whistleblowing by maintaining the security of his project. This showed the extent to how iron-clad Tor's security could be.

The Snowden case reinforced how Tor can be used for good, allowing for benevolent whistleblowing that could not have happened on the public Internet.

Then in 2015 Playpen, a widely used Dark Website for the distribution of child pornography, with as many as 150,000 users at one point was shut down following a collaborative sting effort from the FBI and related agencies in other countries.

Many other news-worthy events have taken place on the Dark Web over the years, including large-scale busts on other illegal marketplaces.

Many believe that as long as there is the need for anonymity online, the Dark Web in some form will continue to exist.

Regarding the security of Tor Project, the most popular service to browse the web anonymously, is under suspicion. Tor Project has suffered from a couple of security setbacks in the recent times. These

included the attacks on Tor and confirmation of the possibility of the security breaches. In 2014, judicial agencies and law enforcement agencies all around the globe rallied against the Tor network services.

There are possibilities of Tor being compromised by the NSA who has called it “the king of high secure and low latency anonymity.” The US department of defense, that includes NSA, funds the Tor Project and in the past, it has tried to compromise its integrity. The NSA has attempted to break the Tor browser’s encryption and has been successful to a small extent.

In past, Tor network has announced that some unknown sources have managed to get the information about people who are using these hidden services. You will need to also use a good VPN service to help stay anonymous.

https://www.soscanhelp.com/blog/history-of-the-dark-web

Author Messages The HUB

FatherTed

- *Vendor*
- *Hero Contributor*
- *Posts: 1989*
- *Community Rating: +409/-475*

Re: (No subject)

« Sent to: n0stis

I can't encrypt to you're key, Don't know why. Anyways there is an emailing system built into the forums but its disabled as it can be exploited to reveal the true IP address hidden behind Tor and this is a security risk for a number of reasons.

There is nothing wrong with any of the terms you used to describe your issue! The mods/admins are clueless on the ins and outs of operating there own forums and then to try and tell others there wrong is just laughable..

This forums has changed hands a couple of times in the last 10 years and current owners literally just about got it hosted and working and to try and update say the themes or something is like trying to put a man on mars for them I wouldn't take much of anything to heart they say to you.

The hidden moderator called "benihana" is the only one with a brain and talks some sense, The other mod called "TPV" just licks the other mods asses and the two global mods one of which is the admin just like to run down the newbies and make out like there some kind of security experts.

You may see me being rude to market operators on here but I actually am a network security advisor and web developer so I am like that to get more in depth answers but I do and agree with you that there is no need to be rude to newbies, A newbie is just an unqualified expert

Quote: "You may see me being rude to market operators on here but I actually am a network security advisor and web developer so I am like that to get more in depth answers but I do and agree with you that there is no need to be rude to newbies, A newbie is just an unqualified expert ;)

Response: Thank you. I have a few questions if you would be kind enough to answer, and I have placed my PGP key below.

My impressions across several months is that the DW I have seen, dread, The Hub, Envoy and a few others are mostly about drugs. Is that a valid impression?

Are there other places you would recommend that I visit to expand my view of the DW?

There is a lot of conjecture in the forums about LE scraping dread. Do you believe this to be real or imagined? Is LE scraping the entire DW?

Do you think that Memex (NSA google) is a real thing?

Here is my public key again in case of some corruption, same as my profile key.

-----BEGIN PGP PUBLIC KEY BLOCK-----

~~ENCRYPTED MESSAGE~~

-----END PGP PUBLIC KEY BLOCK-----

Banned from the Hub and unable to send a PM, n0stis used the email in his PGP key, which looked a bit phony.

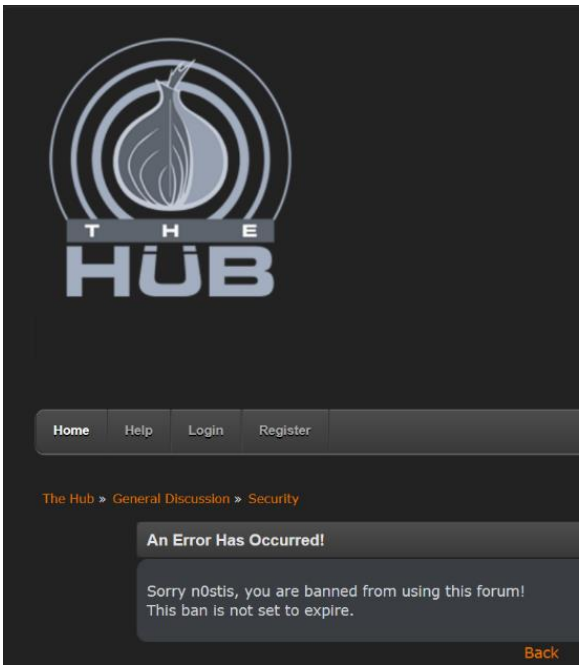
Send this to FatherTed FatherTed@noemail.tor

Banned or not?

I was asked an incoherent question regarding my quoting practices on messages and I responded by saying it was a dumb question asked by a drug addled moron with a room temperature IQ, and then asked if I fit in with the group now. It was the last thing I did there.

He thought it might be phony, and of course it was, as this is the DW after all.

An error occurred : DATA:250 2.1.0 Ok | DATA:550 5.1.1 <FatherTed@noemail.tor>: Recipient address rejected: Relay not permitted. Check out current peering at http://torbox3uiot6wchz.onion/relay-en.php|DATA:250 2.1.5 Ok|DATA:354 End data with <CR><LF>.<CR><LF> |



Ok, so without logging in how does he get this, how do they know his username?

Or is the site just down? Guess we will try again tomorrow.

Am flashing back to my permanent A.User designation on the MS Answer forums from the last book. Banned a dozen times or so as he recalls. Yikes!

Send this to FatherTed FatherTed@noemail.tor address in his PGP key.

Banned or not?

I was asked an incoherent question regarding my quoting practices on messages and I responded by saying is was a dumb question asked by a drug addled moron with a room temperature IQ, and then asked if I fit in with the group now. It was the last thing I did there.

Back to the Hub days later to sign up as a new user arister0s.

The Hub

Registration Successful

Thank you for registering. The admin must approve your registration before you may begin to use your account, you will receive an email shortly advising you of the admins decision.

The Hub »

Login

An Error Has Occurred!

Your account is still awaiting admin approval.

Ok, so I guess that they really mean it about waiting.

The next day all is well with a new username. arister0s. Aristerós is lefty in Greek (just replace the o with a 0).

So all is well and he can send FatherTed an encrypted PM response.

FatherTed,

This is n0stis, banned and back to life, as arister0s.

The Hub snipers got me.

Interesting fun fact. While I wrote a book about my experience on the MS Windows 10 Insider forums several years ago, I was banned a dozen or so times, mostly related to criticizing the product and the Fanbois there. I kept coming back with usernames of the characters in the semi-humorous serial stories I was publishing there and had many fans. That way they could follow, otherwise banned users were assigned a A.User name across the forum threads. There ended up being a lot of those. <g>

I would like to pick up where we left off on our conversation, if we could.

You told me who you were, and I will reciprocate.

I am a writer doing research for a historical novel about the Dark Web. I am not a journalist, but I am looking to have discussions with a number of people on a number of topics on dread, The Hub, Raddle and maybe Envoy.

With my interest in producing a novel with fictional descriptions of who and why people are there and what they are doing, legally. I will also introduce some first person semi-humorous stories within this book describing the hero's quest for a free and safe place in Cyberspace, out of the reach of corporations, governments, and their surveillance and ad driven autonomous algorithmic AI's.

Also because of my extensive technical research, mostly complete, I hope to also produce a technical guide or encyclopedia for both new and experienced DW user community to be housed in the DW Imperial Library collection on

Trantor. Or in this galaxy at:

http://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt26ochei4m6f7tayd.onion/

Now knowing my goals and intentions, what additional or different questions do you think I should be asking? Are the one's listed below the right approach?

- My impressions across several months is that the DW I have seen, dread, The Hub, Envoy and a few others are mostly about drugs. Is that a valid impression?

- Are there other places you would recommend that I visit to expand my view of the DW?

I would prefer to communicate via Tor email, unless you believe that messages in dread are better OpSec, I will let you make that judgment. I am n0stis@mail2tor.com secondarily encrypted or not. Or at arister0s@elude.in

I have no ill intent towards anyone or anything.

Thank you in advance for your participation, and your patience in reading this,

n0stis

I am currently communicating with IaL and Pygmalion and prelim with Rorschach_9000.

Hope I didn't overwhelm you with all of this.

n0stis

Tired of the Hub and Envoy not providing the research value appropriate to the effort involved, and nearing the end of n0stis's patience with this whole DW nonsense, he posted on dread OpSec.

Where and how are Windows OS computers most vulnerable to leak personal IP and ID info?

by /u/n0stis • in /d/OpSec (first message)

Hello all,

While I am most interested in the Windows OS, much of the information in the intelligent, informative, and reasonable discussion I hope to have here will be applicable to which ever particular one of the dozens of Linux variants that those here might be in love with at this particular moment. I suspect some Windows users are quietly lurking here as well.

Now before the misguided, immature, and the trolls begin to denigrate, name call, harass, insult, and make fun of the OP and or the premise of this question: JUST SHUT UP!

Your perceived benefit for doing that is that you may very well learn something from someone here that you can use to your benefit, either now or later. In life it is generally true that if you keep your ears (eyes) busy and your mouth

(fingers) quiet, it will be to your benefit.
For the sake of brevity, assume these two theoretical systems:
One used with a VPN and Tor browser for DW use.
One used without VPN and with Firefox (with security extensions) for CW use
See additional info regarding system hardening in my second message.
With those facts at hand, where are the weak points for leakage?
n0stis
PS. I hope this idea works.

/u/n0stis (second message)
System hardening for the CW with Firefox, and the DW with VPN and Tor
Assume a tuned and hardened Windows 7 bare bones systems. No Win10/11 so No Cortana, No OneDrive. The system used exclusively for the DW, DOES NOT PARTICIPATE IN THE DNM's, (so no conversation about security there is necessary).
This theoretical systems have had the additional numerous hardening steps listed below:
• Tor updated and security at Safest (no JavaScript)
• Tor email only (no IP leak in headers)
• Ahmia search only (no tracking or fingerprinting)
• TMAC for changing (spoofing) your MAC address
• Windows Task Scheduler to disable or delete all unnecessary and intrusive scheduled tasks
• Sysinternals Process Explorer to shut down and disable all unnecessary processes.
• Winaero Tweaker to give you back the system control that MS took away over the years.
• Synchronize with an Internet time server off (should not be necessary behind a VPN)
• Windows NCSI communication across the Internet, EnableActiveProbing OFF (registry edit)
• Paid VPN (passes IP leaks, DNS leaks and WebRTC leaks)
• Zone Alarm for firewall and AV
• SpyShelter anti-keyboard logger
• Spybot Anti-Beacon (kills OS and application telemetry)
• BleachBit for cleaning your system of temp files etc. and keeps it clean
• PGP Tools for encryption and decryption
• 7-Zip for creating and extracting compressed files

•Norton Ghost or other software for image backups to network (NAS) and/or external drives

•An e-Book reader software to read documents

•Quality bios updated gaming router with standard config and NAT

•Wireshark to analyze packet flow from your wired or Wi-Fi network interface. Fix any leaks.

/u/HeadJanitor Moderator

I could honestly give a multi-hour lecture. But I will spare you and tell you to look up Microsoft Telemetry.

/u/n0stis

Well that seems like a dodge to me. Clearly if you read my second message I am aware of telemetry. Let us raise the level of this discussion, OK?

/u/n0stis

Is telemetry network traffic encrypted?

Wireshark will show only unencrypted packets.

Microsoft's Windows 10 telemetry this is encrypted using TLS v1.2, and so there's no way of actually seeing the content of a telemetry packet.

Windows 10's telemetry is not sending vast amounts of your personal data - it's sending small snippets of information to a set of servers with names and IP addresses that can easily be blacklisted at a router if you really want to keep your network traffic private. Remember that not all packets contain data.

hxxps://www.zdnet.com/article/windows-10-and-telemetry-time-for-a-simple-network-analysis/

/u/HeadJanitor Moderator

All of it is it okay if you're okay with it---I mean it.

/u/n0stis

Another dodge? If you don't know, just say you don't and maybe someone else will jump in.

How much Linux telemetry are you comfortable with?

hxxps://linuxfoundation.org/telemetry-data-policy/

hxxps://thenewstack.io/linux-foundation-introduces-a-telemetry-policy-for-all-projects/

Switched to Private dread messaging in an attempt to solicit more info.

/u/HeadJanitor Moderator

Quote: You can use full on links. I can get off in a few hours. Maybe we can connect then. Bring the info out here to for the sake of harm reduction.

Response: Am unclear on what you mean.

URL Defanging is a good habit.

Remember that my question regards both CW and DW OpSec.

n0stis@mail2tor.com

/u/HeadJanitor

I think i meant to educate the masses on Telemetry as a subject as most are unfamiliar with it and that there are numerous programs from easy to advanced that can curb MS Telemetry. I made a "hard reduction post" showing how simple it was using WPD, for example.

/u/n0stis

Well, it worked because WPD is new to me so I will play with it.

WPD Posts

Commented on: Rate my OpSec?

/u/HeadJanitor in /d/OpSec

Disable all the Telemetry features. That stuff is a nightmare. Use WPD and disable EVERYTHING.

Commented on: Jump from tails to Whonix

/u/HeadJanitor in /d/DarknetMarketsNoobs

Download a tiny file called WPD (program name)

It's a small zip file.

Extract it into "WPD"

Disable everything going downward.

Commented on: Jump from tails to Whonix

/u/HeadJanitor in /d/DarknetMarketsNoobs

Make a folder in your C drive called "WPD"

Commented on: Surveillance Capitalism | Blocking Telemetry in Windows | "Harm Reduction"

/u/HeadJanitor in /d/OpSec

If you get stuck along the way let me know and I'll help.

Make a folder called C: \ WPD

Empty the contents of WPD in there and go to Privacy.

Start sliding everything off, disabling them.

Surveillance Capitalism | Blocking Telemetry in Windows | "Harm Reduction"

by /u/HeadJanitor previously in /d/OpSec

*...Bundle Private WinTen Blackbird v6 O&O ShutUp10++ WPD - Windows Privacy Dashboard WindowsSpyBlocker Spybot... Download WPD - Windows Privacy Dashboard Uncheck ***everything*** from top to bottom. https://wpd.app/ ... that can be done to stop the leakage --- start with WPD...*

Privacy dashboard for Windows (WPD)

A small but powerful portable tool that works through the Windows API. WPD is the most convenient way to configure various privacy settings in Windows.

https://wpd.app/

Surveillance Capitalism | Blocking Telemetry in Windows | "Harm Reduction" (cont.)

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/5fdcc7ce6e389f72be0a

Quote: Telemetry is a necessary evil, as software developers need to collect data to be able to improve their products to sell you what you think you need by taking into account your actions, the things you do, the things you type in Google, the number of times you visit a site, the things you bookmark, the routes you travel. The minute activities that make you who you are and the things that subliminally grab your attention and bring you to focus.

For us, as Tor users in the Dark Net, it's outright dangerous to have our computer activities logged and sent back as "telemetry".

/u/n0stis

Response: I would suggest that it is both NOT a necessary evil and is equally dangerous on the CW. We did just fine prior to 2012, when a new term was invented in Silicon Valley called MVP or Minimally Viable Product. The new mantra was ship it if it kinda works and start the cash flow, then send updates to do the fixes. Users become your beta testers, so you can fire or redeploy all that testing staff and save a ton of money. Maximize your shareholder value!

Quote: (And know that with each update Microsoft tries to un-do our reversals.)

Response: And here he makes my case of not using Windows 10/11 and forcing updates off on Win7.

Ask yourself if you have had more computer problems due to lack of updates, or _because_ of updates. Industry wide FUD for profit going on here.

/u/n0stis

Quote: "they came here for drugs,"

That is a pretty big generalization.

Are you saying that dread is primarily for drug seekers?

/u/HeadJanitor Moderator

Just from my vantage point of collecting 30+ messages a day: 24 drugs, 6 carding. I personally don't go to the marketplaces but what I meant to imply is myself and so many others have tried to instill basic Linux (speaking, PGP skills) and that's not their concern. They're here for an objective and very rarely have I met someone who stopped along the way to pick up skills on an operating system they don't use at work or school.

/u/n0stis

That is believable that they don't come specifically for Op-Sec skills, but they do learn that they need some in the process, yes?

I just thought that there might be a reddit like social aspect to activity here. Knowledge seeking, conversation seeking, venting, etc.

/u/AbraCadaver P

The Microsoft Windows operating system talks to ***291 hosts and 2,764 IPs*** *on the internet. List of URLs & details below: https://helgeklein.com/blog/windows-os-services-apps-network-connection-target-hosts/*

/u/n0stis

Ok, so which of these would reveal system IP's or ID's?

Did you read the second message regarding beacon blocking, process and task blocking, etc.?

Btw, I picked this up over on Envoy, views from two OpSec experts.

/u/n0stis

In reviewing the document you linked to, it is clear that this is Win10 data from systems not disabled or modified in any way. It is also unclear and unexplained what the meaning of this information actually is. So what is _your_ intended meaning by sharing this information with me?

/u/n0stis

So all OS's need hardening right?

Securing Debian Manual 3.19

This document describes security in the Debian operating system. Starting with the process of securing and hardening the default Debian GNU/Linux distribution installation.

hxxps://www.debian.org/doc/manuals/securing-debian-manual/index.en.html

Some Simple? Whonix Security Hardening Steps

Response: This reads like a Russian novel...written in Greek

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/36134b759eacb6ddc8c8

/u/HeadJanitor Moderator

*Crap. I'm just seeing this. Feel free to use full URLs here. I've played with all four tiers of Microsoft's Telemetry. I understand it's just business. They're not out to harm me. To be honest, I'm stick of the subject matter because I've spent so long on it. And a part of my "job" is to *briefly* inform others, otherwise what good would I be. Now I can't past a thesis here but I can explain 'just' enough for them to decide. In the end, their decision is their own.*

/u/n0stis

My original intention, as explained in my first post, was to have a far reaching intelligent discussion of CW and DW Op-Sec. This has failed miserably on this sub.

Flippant quotes like don't use Windows because of telemetry, are no different than saying don't use Tails because Snowden doesn't, or because if you configure it wrong you put yourself at risk.

Decisions made on incomplete information will not lead to good decisions.

I have made another couple of posts to try to redeem this subject.

Or perhaps I am in the wrong place to do this.

/u/HeadJanitor Moderator

No, you're in the right place. Just throw in examples for each point you're trying to get across. There are currently three people to whom I am 'explaining' what Telemetry is, its source and purpose---like a child pointing at an object, they just wanted what they wanted. We need to elevate the subject matter and there are many who will gravitate toward it, but not the majority.

Not having had a lot of luck in stimulating conversation around security in /d/OpSec, n0stis thought he would try again with a couple more questions.

I would seem however that at this point in time that it is not possible to have a reasonable intelligent discussion on the most important subject on the DW, OpSec, in the most relevant sub on the largest and most active forum on the DW /d/OpSec. We shall see…

Is anyone using a Mixnet?

by /u/n0stis • in /d/OpSec

Is anyone using a Mixnet, like Nym, to get network level privacy that protects your IP even against the most powerful, passive adversaries with large scale traffic analysis that can observe every packet going in and out of your Internet connection?

Mixnet nodes achieve stronger metadata protection by reordering the messages they route, in addition to transforming them cryptographically. This makes messages untraceable both in terms of appearance as well as timing. Mixnets

in theory, provide stronger metadata protection than VPN's, Tor or any of its peer-to-peer alternatives.

Too complicated?

Too untested?

Too expensive?

Never heard of Mixnets?

2 comments

/u/Hungry_Eyes 1 points

First I've heard of mixnets. I'll do some research and think about the subject. While it sounds good, it also sounds as if it would attract the attention of TLA's[51], which is opposite of the purpose of using something used a lot, such as TOR and VPN's.

/u/n0stis

nymtech.net is a place to start. Also anything said or written by Gavin Wood or Harry Halpin.

So thus far, we have an acknowledgement of ignorance on the subject but yet an opinion is easily proffered. Not a good start.

/u/Anonymator59

So basically like a tumbler but for data instead of coins? That does sound interesting but I'd assume both the user and the server need to use the mixnet for it to work

/u/n0stis

Yes and no. A random shuffling of a deck of cards, I would explain it as. You would vpn or dvpn (to conceal your entry point) into the mixnet (nothing on the client side). Anonymity would depend of the size of the number of nodes in the mixnet but I believe there is a way to introduce junk packets (chaff) into the system if the threshold falls below a certain point. It can use decoy traffic (these dummy packets), timing obfuscation (stop and go delays) to prevent interception of the packets.

In a mixnet the nodes store the ledger but NOT the data.

Tor suffers from a lack of nodes and geographical diversity, and has less metadata protections.

Then a misunderstanding from the same dope, and an acknowledgement of ignorance of the subject from another.

Anyone using decentralized VPN's?

by /u/n0stis • in /d/OpSec

---

[51] *Three letter agencies, FBI, CIA, NSA.*

What about decentralized VPN's (dVPN) such as Orchid or Sentinel?
Too complicated?
Too untested?
Too expensive?
Never heard of them?
3 comments
/u/Hungry_Eyes 1 points
Is this the same as the mixnet post you made a few minutes ago?
/u/n0stis
Completely different subject.
/u/TheRichBarber 1 points
Never heard, but I'll look at it.

So I did not get very far to this point with my two questions towards a deeper understanding of DW OpSec, and I do not believe it was related but then this popped up:

Hitchhiker's Guide to Anonymity
by /u/Pygmalion Vendor Opsec • in /d/OpSec
Dear Community,
This is now your homework. Read all of https://anonymousplanet-ng.org/

Note: A search to uncover the general identity of the author(s) revealed this link:https://www.reddit.com/r/privacy/comments/t83zz6/does_anyone_know_what_happened_to_anonymous_planet/

Then come back here and ask your questions in /d/opsec together.
Study this together as a community and help each other on the level discussed on that site.
/u/HeadJanitor and myself will read all of your posts and step in if you guys get it wrong, but please try and figure the stuff out among yourselves.
You will be recognized opsec experts. Licenses will be given out by /u/HeadJanitor for a small fee in exchange for his time and efforts (yea, testing your knowledge is work and you need to pay, so quit bitching). People who graduate will be recognized and Darknet licensed opsec experts. You will receive a PGP signed message and a flair here in /d/opsec and /d/vendor_handbook.
Thank you.
Sincerely,
Pygmalion

/u/donkeysquadreborn

u got onion 4 that site little P??

/u/We_Are_9000 Paranoia Level

Are you scared of the surface web????

If so, get the fuck over it!!!!

Why???? This makes zero sense!!!!!

Are you Howie from The Bench Warmers????

Do you also hide in the closet & eat sun screen????

Come Out Of The Closet!!!!

/u/Pygmalion Vendor Opsec

Ah man you trip me up. xD

/u/We_Are_9000 Paranoia Level

Well, if these fools would take the time to learn real OPSEC & use it everyday, there is nothing to fear on the surface web.

If you guys have not added Kodachi to your OS list, you really need to, it makes Tails look like a bowl of cold oatmeal. You should check out its versions of Firefox, total lockout of the so called things to fear.

Where did common sense go? Because that is a very important part of staying safe online, surface web or darknet.

/u/yosegi

I documented myself and I tested kodachi unless I am mistaken kodachi is dangerous, I made a post /post/4e47647666965d811e05

if I summarize kodachi obliges to use his vpn before tor then obliges to use his dns after tor moreover in their condition kodachi declares to collect your ip address as well as your hardware address

"I pay monthly rent to run the VPS nodes and utilize them for VPN which is provided to you, I do not collect ANY data or store ANY information (Logs) that belongs to the user except the hardware ID (hash) and connected IP address (VPN IP) that has to be sent automatically when your PC establishes a connection to the VPN. This information will only be used to banned you from the VPN nodes if you have abused the bandwidth or I received complaints of hosting torrent files. If that is the case you will be banned permanently Kodachi is provided for anonymous surfing and not for heavy daily file and movie downloads.If you think you have been banned by mistake please send me your Hardware-ID via contact Discord and yes you can use your own VPN then no HWID will be sent to the server."

I confess to not understanding to see kodachi regularly quote as a good OS whonix is a very good compromise and remains accessible to use qubes if we have the will to understand its operating logic, I find it less complex than we think

/u/Pygmalion Vendor Opsec

Kodachi is fucked because it is based on a distro that will no longer receive security updates soon.

Other than that it's really good, but yea, it will be out of date soon unless they step up their gears.

/u/We_Are_9000 Paranoia Level

I can't see that upgrade not happening, its the same as not updating Tor itself. I'm certain that shooting themselves in the foot is not on the table.

/u/alwaysfire

Quote: "If you guys have not added Kodachi to your OS list, you really need to, it makes Tails look like a bowl of cold oatmeal."

Response: In terms of "features", Kodachi does make Tails look like a bowl of oatmeal. However, with more features comes more attack vector, more possibility for human error, and more possibilies for bugs, misconfigurations, etc. Kodachi is also produced by one single developer, who stores his public pgp signing key in an impossibly hard to find place. Placing all that trust in one single dev isn't a great idea. Without many eyes and oversight, it's prone to have many more security issues than tails. It also uses the developers free vpn service as a default vpn. Using any free VPN is a bad idea, and bad for opsec. I agree that kodachi has many more features than tails, but I strongly dissagree that It should be used over tails. Tails is idot proof and kodachi is not. Theres a lot that could go wrong with kodachi in terms of opsec.

/u/We_Are_9000 Paranoia Level

By default a dis-service is being done by not pushing everyone to learn a more difficult OS that offers more in terms of security. When is learning anything new a bad thing?

If i can become decent at Qubes, trust me, then anyone can. When i found the DNM sub on Reddit all those years ago I was BEYOND green behind the ears in terms of OPSEC, using just Tor with Windows. Now I keep 2 machines one with Ubuntu & one with Qubes, both with Whonix.

We face an enemy that we actually pay to hunt us down & throw us in jail, so the more we know about keep ourselves safe, the better off we are.

One slip up is all it takes to end up in a cell with Tyrone & his 13 inch BBC!!!!

/u/alwaysfire

Quote: When is learning anything new a bad thing?

Response: I think you already answered your own question here...

One slip up is all it takes to end up in a cell with Tyrone & his 13 inch BBC!!!!

Ultimately, Learning, isn't a bad thing, however, if a small error or misconfiguration you made but don't have a full understanding of yet, could put you in jail, then, learning has to be done strictly within the confines of a home or private network. NOT ONLINE! But that is really hard to

accomplish, since, well, you really need to be online to see how things actually work.

I agree with you that we need to push people to learn better technologies, especially noobs. However, we also have to come to terms with the fact that at least 25-50% of noobs don't have the will, or the time to learn more sophisticated technologies, and how to safely implement them. Thats the beauty of Tails. It is the best OS for the Mainstream Darknet users. It prevents them from fucking up big time. I mean, even most experienced vendors I've talked to don't know anything but the very basics of online opsec. I'm mostly in agreement with you here, that we should push others to learn better technologies. But I also am a realist. And realistically, noobs are never going to go away. There will always be a big stream of them coming in and not knowing their opsec, and not having the will to understand good opsec. So for them, tails is the way to go, to protect them from their own ignorance and stupidity. Not everyone who uses the darknet is going to try to level up their opsec. We just have to accept that.

/u/We_Are_9000 Paranoia Level

While I don't disagree with anything you have said, in this, as well as everything there is the low hanging fruit.

I've said this a thousand times, this shit ain't for everyone.

/u/KyleKlemons54

I completely agree there man. It's fucking ridiculous - the exit node in Germany, Estonia or wherever in the world wouldn't find this website to be "sussy" in anyway (and besides - it's pretty sussy that this poster here LEGIT thinks accessing a normie net site to be "sussy").

/u/Pygmalion Vendor Opsec

Are you really that lazy?

Go get it yourself.

/u/donkeysquadreborn

aight damn little P y u sweating me? jus tryna help the noobies out dawg smh didnt know u were like dis

/u/Pygmalion Vendor Opsec

My apologies. Just short tempered right now because a bunch of people are stepping on my shadow.

/u/donkeysquadreborn

it aight dawg hang in dere we all have bad dayz xxo

/u/heraykay47

Thank you, opsec comes first

/u/We_Are_9000 Paranoia Level

FYI.....Tails is NOT a tool for anonymity!!!!

You guys really should start real education that benefits people!!!!

Just Saying :-)

/u/ShulginIsMyGod

also, /u/pygmalion do you care to comment on this? I get the spirit of this guy (also, kinda like it, ngl) and/so I'm not entirely sure about this. why is he shilling W this hard against Tails? do you guys think he's got a point?

/u/Pygmalion Vendor Opsec

It was discussed at length. Please study my profile and my post history because I don't wanna repeat myself.

You can probably find it with the search function.

Feel free to shoot any new questions I haven't answered yet. :)

What I will say right now is that Tails is on the list of recommended operating systems for darknet operatives. Just to be clear.

edit: Gave them the appropriate user flair.

/u/ShulginIsMyGod

yup, I followed some discussions on here, didn't think to have read your personal comments on the matter so I wanted to hear yours directly, now I'll search for it, ty, man

/u/We_Are_9000 Paranoia Level

Tails is great if you are in China or live in a country that is anti freedom. By its design it leaves no trace on your machine.

As a matter of fact, its what Edward Snowden use when leaking everything he did. But now he is a big supporter of Qubes.

Tails is open to the same attacks as just using the Tor browser.

Using Whoinix inside of whatever VM prevents leaks, man in the middle attacks, it is considered much more secure by the real experts. When used in Qubes it is as secure as we can get.

Like I said above, Tails is not built to hide your real IP address, its basically computer camouflage, with no walls to protect the castle. So claiming its a tool to hide your IP address is false.

Tails or Jails.....Total fucking bullshit!!!!!

No safer than just using Tor on a Linux distro!!!!!

/u/n0stis

Right. Like saying that your IP remains in the Tor metadata. Right?

/u/We_Are_9000 Paranoia Level

It's a know fact that tor by itself has exposed the real ip address of users.

Whonix prevents that.

Note: Whonix:
An alternative to Tails and an open source project. Whonix is an operating system focused on anonymity, privacy, and security. It is based on the Tor anonymity network, Debian GNU/Linux, and security by isolation. DNS leaks are impossible and not even malware with root privileges can find out the user's real I.P. address.
Official Site: https://www.whonix.org/
Whonix For The Darknet Markets: http://archivecaslytosk.onion/COfTH

/u/ShulginIsMyGod
/u/Pygmalion Vendor Opsec
Just living up to Circles of Revolution.
/u/gencoch
Please don't jump on me. We all have to start out somewhere.
Do I need the 'Darknet Bible' in addition to this document, or is 'Anonymity' enough?
/u/Pygmalion Vendor Opsec
This is a science project and far superior. The bible is obsolete in my opinion.
/u/mousetrap
Thanks for the guide.
P.S. I have also learned how certain people feel about oatmeal.
/u/KyleKlemons54
Thank you very much for this. Much appreciated.
/u/sleevo
1 points
I will be reading this now I meant to before but I forgot I will be back in how ever long it take to read 400 pages
/u/COJOD
Thank you! Challenge Accepted!!!

Of course n0stis not being able to resist, provided some initial commentary on this proffered document in the OP (original post).

by /u/n0stis • in /d/OpSec
First of all, I would like to say that I fully appreciate the effort of the writer(s) who brilliantly put this document together. As near as I can tell they remain unidentified and go unpraised. But I just did here.
Because it is a many days long slog to work my way through this document, if

I actually make it, my first comments are not regarding content but on User Interface or UI. These comments reflect the pdf version read in (a communications crippled) Adobe Acrobat in Read Mode zoomed to fill the 24 inch portrait screen at a 1080x1920 resolution. This being probably one of the most ideal screen reading environments currently available. Many people including myself, have difficulty reading long documents on a screen and typically print them out. This should be taken into serious consideration here.

The writer is clearly a technologist and not a typographer or graphic design artist as the text typeface is somewhat faded and difficult to read, and the graphics all seem to require zooming in to read them, and seem to be randomly sized and arranged in a not easily readable form. A project of such importance and magnitude, not to mention the significant existing effort that was expended in writing this, deserves some additional attention to properly bring it home comfortable to the readers eyes.

Beyond the UI, the writer(s) is clearly not an academic as the organization and structure are too scattered and would be much better in an organized chapter form. In addition, the services of a professional editor would be welcomed here as well. For example: I would like to see some information structured by access device type and by geographical location. This would make the information more accessible by being able to ignore what is not specifically relevant to each individual reader. For example: I, like Richard Stallman, Dave Eggers etc. do not use a smart (sic) phone, aka a cellular Newton. Nor do I live under a repressive government, well at least under the common understanding of that phrase.

The document also suffers from the lack of a page numberes and a more clearly identified hyperlinked Table of Contents. A TOC and an Index are also quite easy to generate these days in adequate word processing software.

All of this is to say that a reader, however well motivated and well intentioned, must be drawn into the content and not repelled from it. This should be a more rich text document with color and formatting that are inviting to the reader. Graphical notations for Tips and Tricks and Notes could be used to catch the eye of the reader. The web links in the body text and footnotes should be hyperlinked, even if url defanged.

The footnotes at the bottom of pages, rather than at the end of the document, are welcomed and useful. The Archive.org, Wikiless, Scrtibe.rip, and Invidious links are a very good idea.

This review is not unlike something I would give a Kindle book on Amazon. Although with the Kindle sausage grinder text and graphics conversion, there is little the author can do about its inherent flaws, except to pass on it.

Regarding content, some searches of the document have revealed that it does not contain any information regarding mixnets or decentralized VPN's (dVPN).

I have shared all of this experience/information/opinions with the writer(s), but thought I would also share them here for the benefit of those who seek to document important information in writing for posterity.

PS. A quick search to reveal the author(s) uncovered these links:

https://www.reddit.com/r/privacy/comments/t83zz6/does_anyone_know_what_happened_to_anonymous_planet/

The 22 year old OP has apparently died in Ukraine, at Russian hands, and another has taken over the project and is fund raising for burial costs:

https://anonymousplanet-ng.org/donations.html (NG is the country code for Nigeria) https://anonymousplanet-ng.org/about.html

Now in retrospect, this makes me feel creepy having written the above critique.

RIP, Lena

The email outlining my thoughts on the above document to contact@anonymousplanet-ng.org bounced, so wandering over to GitHub n0stis found an issues topic to post to. He got the following response:

From: Than Harrison [mailto:notifications@github.com]

Sent: Wednesday, June 15, 2022 6:14 PM

To: NobodySpecial256/thgtoa <thgtoa@noreply.github.com>

Cc: Lefty-Insider Author <author@noreply.github.com>

Subject: Re: [NobodySpecial256/thgtoa] Document construction (Issue #31)

Thanks for the acknowledgement. A ton of work is being put into this and nobody is being paid to maintain it.

One thing I recently started work on was chapter pages. It would make it more easily accessible and feel less bulky. The code is hosted off the main line. I also plan to create a better bibliography to make it look more like an academic paper. The LaTeX is a bit bulky so it's not expected to be published online until I know it compiles. I also need to find a way to better render the images in the PDF because Kramdown doesn't like to display them the way the reader would find comfortable. Kramdown doesn't like formatting in some areas, behaving poorly and ignoring it altogether in others.

The goal is to work on the ability to create a clean light and dark mode PDF style. The website and PDF are the things we are focusing on at the moment because they are the most viewed. Not many people are coming here to discuss changes they would like and it's why we have so little plans to change many things. We won't change it if it's not presented to us. As a technical writer, I see your concern about the accessibility. I'm sort of new to the way this is being done. I've already considered forking it into a new style that builds directly

from LaTeX as I am comfortable with that and it offers more options for the UX. The other concerns I have include the logo, which I've been working on as well.

The guide doesn't include a mobile user in its model because using a cellular device is not recommended for privacy. I don't use a cell phone. I don't know any reason you would want to use one and you have no expectation of privacy without severely limiting usability and function. I emulate Android and I only use it for specific apps. There are already tons of guides for mobile OS users and they include several things such as compartmentalization, anonymization and security. It's outside of the scope of the guide for those reasons.

I have already started splitting it into chapter form and setting a bibliography. The rest are soon to follow. We could benefit from more technical writers and even some developers that are familiar with making specialized web pages, so the reader can pick between certain sections and it doesn't feel so overwhelming.

Reply to this email directly, view it on GitHub, or unsubscribe.

You are receiving this because you authored the thread. Message ID: <NobodySpecial256/thgtoa/issues/31/1157062879@github.com>

From: Lefty Insider

Sent: Thursday, June 16, 2022 11:32 AM

To: 'NobodySpecial256/thgtoa' <reply+AZUIAX4FNIA467XKL5PNBAOAW6NDZEVBNHHEXRZDV4@reply.github.com>

Subject: RE: [NobodySpecial256/thgtoa] Document construction (Issue #31)

Than,

Thanks for the acknowledgement of a response.

I originally found a link to your document on the DW dread OpSec forum where I am /u/n0stis in /d/OpSec doing book research.

I posted the same The Hitchhiker's Guide to Online Anonymity Preliminary Review info there, in an effort to improve the writings on the DW in general and those related to operational security specifically.

The LaTex you use is unfamiliar to me as I am accustomed to a WYSIWYG environment in MS Word. While not the ideal document production software, I can remember Ventura Publisher fondly, Word has allowed me to produce stellar pdf's of the novels listed above. I have no need to publish in any other format, or to batch process anything. I see myself as a document artist and want to individually touch each word and graphic, and craft each page individually.

I don't know what Kramdown is, but it doesn't sound good. Reminds me of the word and text conversion sausage grinder that creates Kindle books.

I am busy writing two books now, but would not be disinclined to provide your org with some technical writing assistance if I can.

Lefty Insider (arister0s n0stis)

So n0stis aka Lefty thought all was good. He had provided some unsolicited feedback on the document in question and it was well received.

Since he had signed up to revive new posts on this issue, some new unsolicited messages starting coming to that were less well intentioned.

From: Alex Anderson [mailto:notifications@github.com]

To: NobodySpecial256/thgtoa <thgtoa@noreply.github.com>

Cc: Lefty-Insider; Mention <mention@noreply.github.com>

Subject: Re: [NobodySpecial256/thgtoa] Document construction (Issue #31)

I'm aware of the issues with the PDF styling. These issues are inherent to the toolchain used to build the PDF from Markdown. The Cyrillic characters not rendering in the PDF is a known issue. It's due to the fact that Pandoc doesn't support non-ASCII character sets.

As for the formatting, the document was written over the course of multiple years and as such, has developed a complexity not dissimilar to the evolution of a codebase over time. We can begin reworking the structure of the document if people think that's important enough.

So Lefty learned here that this publication is being processed in a batch, not unlike compiling computer code I suspect, by a series of software tools (an open source toolchain) which have some shortcomings.

And then some qualifications on my document format/structure suggestions and for adding content:

The guide doesn't have much in the way of page numbering, partly as a limitation of the toolchain, but also because it's intended to be read in digital form, as opposed to printing it out on paper. I'm not sure there's enough reason to change this, but I'm open to seeing if some people feel strongly enough about this to justify the change.

This isn't an oversight, it's a safety precaution for higher-risk readers. The guide tries to only recommend solutions that are known to work. I'd rather give people a small set of trustworthy options, as opposed to giving people a large set of less-proven options, which could put certain readers at risk if the recommendation turns out to be premature.

From: Lefty Insider

To:'NobodySpecial256/thgtoa'
<reply+AZUIAX3DWCUD4LDZGVGFBHWAXPTJLEVBNHHEXRZDV4@reply.github.com>

Subject: RE: [NobodySpecial256/thgtoa] Document construction (Issue #31)

So far, you have identified multiple limitations of your toolchain. Makes you wonder. It seems that your automation tools are limited and are perhaps overkill for such a relatively small document.

Anyone reading the "guide" could site numerous occasions in it where multiple solutions are provided, allowing the user to decide based on individual circumstances. Everything in this document identifies privacy solutions, which work to some extent better than others. E.g. VPN over Tor or Tor over VPN, bridges, choice of OS, etc. So this comment is a bit disingenuous in my view.

> *From: Than Harrison [mailto:notifications@github.com]*
> *To: NobodySpecial256/thgtoa <thgtoa@noreply.github.com>*
> *Cc: Lefty-Insider; Mention <mention@noreply.github.com>*
> *Subject: Re: [NobodySpecial256/thgtoa] Document construction (Issue #31)*
> *This is currently in the scope of a non-public body of work I am working on in my spare time to convert the document entirely to a LaTeX style so it can be automatically built into a PDF, still using Pandoc, but in a more accessible way. There are many known issues in the conversion including the Russian style writing not being rendered and the ToC not working as expected in some areas. The format of the ToC is also jumbled. I didn't bother making this public because it's a long rewrite and almost would require being its own fork and I can't simply do that because it would be without signatures and I have no intention to take over the project since I am just a contributor. Pandoc conversion is the route the project has taken so far and I aim to keep it that way with minor modifications including rewriting into chapters to make the document easier to edit and maintain.*

Ok, so now I am starting to understand that this document is being treated, as a coding project would be, is suspect, complete with author signatures. The checking in and out of words. (code) Lefty not being a coder and being new to GitHub is definitely a noob here.

> *I also would like to point out that, on the subject of format, you should not be quoting the entire email in your reply, as it is adding weight to the page, so please try to reply without quoting the entire post above.*

Per the link at the bottom of each email response he received, Lefty responded via email.

> Reply to this email directly, view it on GitHub, or unsubscribe.
> You are receiving this because you were mentioned.

So Lefty started to clip his email quotes tighter and got this:

From: Than Harrison [mailto:notifications@github.com]
To: NobodySpecial256/thgtoa <thgtoa@noreply.github.com>
Cc: Lefty-Insider ; Mention <mention@noreply.github.com>
Subject: Re: [NobodySpecial256/thgtoa] Document construction (Issue #31)
Tl;DR - quotes the entire thread yet again, making it unreadable for anyone
Basically just said it makes it hard to read when you format it this way.

Yet he is not formatting anything, just using Outlook for email messaging. Then things started getting really nasty and defensive.

From: Alex Anderson [mailto:notifications@github.com]
To: NobodySpecial256/thgtoa <thgtoa@noreply.github.com>
Cc: Lefty-Insider ; Mention <mention@noreply.github.com>
Subject: Re: [NobodySpecial256/thgtoa] Document construction (Issue #31)
Are you going to offer anything but snide remarks about the body of work or are you going to open a PR and contribute changes you'd like to see? Cause I'm going to have to block you if you reply using the full text. It's very annoying. You're complaining.

So what is a PR? Use the website to create an issue? Which he did. He is soon to find out more however.

If it's too opaque, allow me to make it clear. The guide maintainers can take your criticisms and apply them to the body of work as we get to them.

If you'd read this project's contribution guidelines you'd know contributions are submitted in the form of pull requests. If you submit your changes as PRs I'll be happy to review and merge them. Please open a new Pull Request or Issue and address your exact concerns there, sticking to the style guide and contributing guidelines.

If you want something mentioned, you should be prepared to justify why it's worth mentioning. Alternatively, you could ask nicely I might do that research for you. Not doing your own due diligence, is an easy way to get yourself ignored.

When opening an issue you're requesting the maintainers of a project to do something. The least you could do is explain why you think it's a good idea. And when contributing to a project there are guidelines you're expected to follow. And if you can't be bothered to do those basic things, the least you could do is be respectful to the people you're asking pick up your slack.

The fact that you're writing from Outlook is exactly why your posts have had issues (this isn't an email chain, it's a GitHub issue. I figured you'd have noticed that by now but apparently not).

Ok, so some more limitations of open source software. Looking directly at the website, no formatting issues are visible. And then apparently they collectively decide to take further discussion off into a restricted arena.

Yeah, this issue really should have been split into multiple issues to begin with. Let's discuss the rework further on Matrix. Closed Issue #31 as completed.

Lefty could not resist but offer a bit more of advice for these youngsters.

Your obsession with free and open source software ensures that you will always be using substandard software and having problems obtaining reliable and quality output. You can buy good tools at Sears or cheap ones at Harbor Frieght (or perhaps old ones at a yard sale). I am writing these emails from Outlook, clipping my quotes and apparently your software (GitHub) has a problem with seeing that as well, despite the invitation to respond by email at the bottom of each message.

I provided you with what I believe is some valuable input. What you do with it is up to you. I never offered to be your technical writer or researcher or to convince anyone of anything.

I am plenty busy, so I won't engage in this silliness here any longer.

There is really no good reason in my view not to mention certain privacy and anonymity technologies even if your review of them is negative. Open your minds, the future is hard to predict.

IBM introduces the PC and, with Microsoft, releases DOS ("640K ought to be enough for anyone" — Bill Gates 1981) https://quoteinvestigator.com/-2011/09/08/640k-enough/

"Residential services will depend on high-speed Internet access. High-speed today is 100 Kbps to 900 Kbps. This will increase in the future to 1 Mbps to10 Mbps for each household." https://www.pearsonhighered.com/assets/-samplechapter/0/1/3/0/0130281360.pdf

"We don't like their sound, and guitar music is on the way out." — Decca Recording Co. rejecting the Beatles, 1962. https://quoteinvestigator.com/2013/04/27/guitars-out/

Open Source= everyone can look at the code, but few actually do. Kinda like the shared car that everyone drives, but no one puts gas in.

A bad workman blames his tools (an old, French proverb that dates back to at least the 13th century)

I am not sure how the wheels came off here, it may be communicating with foreign nationals where English is a second language, coders fulfilling the stereotype of being socially inappropriate, or it may be just geeks being rude.

Lefty accepts the responsibility for not knowing the rules in this domain, however well-intentioned his comments were.

I live in an html rich text world. If you guys want to live in the stone age and bad old days of plain text fine. I will format this message as plain.

You want to use substandard open source software because of some bias against commercial software fine. Just count me out.

If you want to beat up on someone well intentioned, but uninformed of your cliquish and socially inappropriate ways, that's fine with me.

"Hey, the 90's are calling you guys and they want their Courier New back."

PS. I have been posting publically since CompuServe and 2400bps.

So to contribute to the ongoing operational security discussions on dread OpSec, n0stis, you remember him right?, posted a couple of additional messages. He is still looking for some reasonable and rational discussions.

/u/n0stis in /d/OpSec

We all know that CW Webmail sucks, even OWA. We also know that DW Tor email suffers from a lack of interoperability, server uptime (I'm talking to you elude) and .general ugliness and clumsiness.

What we need is an Outlook-like client for the DW!

What if there was an email client, which allowed the importation for PGP keys, and ability to interoperate with onion addresses and encrypt/decrypt seamlessly.

When you send an email it would ask Clear text or encrypted and at what level? Then ask you which PGP key to use. When you receive an email it would be automatically decrypted by your PGP key. The recipient would simply need to import their keys to read and send. Encrypted messages in your In, Out, and Sent boxes would be marked as green to identify them as such.

You could send your public key with your message, or send encrypt invitations much like Outlook Calendar invitations now.

What if you could Keep the NSA Out of Your Inbox? Anyone monitoring the email would be able to see the size of the message but that's about it. If sent over a Mixnet, not even that will be seen.

https://darkmail.info/downloads/dark-internet-mail-environment-march-2015.pdf

/u/n0stis in /d/OpSec

What is a Mixnet?

It is a decentralized network that uses blockchain technology to mix and scramble packets of metadata — e.g. your IP address, who you talk to, and when and where. It is the successor to privacy technologies like the Tor browser and VPNs.

It acts as a network layer 0 Super VPN to mix your packets with others so that they cannot be individually identified, even by intelligence agencies of a nation state actor. It eliminates any fingerprints like randomly shuffling a deck of cards.

Differently from onion routing, however, mixnets route each individual message independently. What differentiates mixnets from Tor and peer-to-peer networks is that mixnets are designed to provide metadata protection from global network adversaries. Mix nodes achieve this by reordering the messages they route in addition to transforming them cryptographically. This makes messages untraceable both in terms of appearance as well as timing. Mixnets thus provide stronger metadata protection than a Tor/VPN combo, or any of its peer-to-peer alternatives.

https://nymtech.net/nym-whitepaper.pdf

It seems as though /u/HeadJanitor (/d/OpSec Mod) in a private encrypted message, and /u/n0stis's thoughts were prescient on their concerns about Pygmalion recently being made a co-mod in /d/OpSec.

A public enterprise business? What does that even mean?

Interest Check: Opsec Guide for Mobile Communication

by /u/Pygmalion Vendor Opsec in /d/OpSec

Dear Community,

/u/HeadJanitor and I would like to write a full on security guide about mobile communication.

Real world professional darknet operatives require constant communication just like everyone who is working as a team full time.

Therefore we need a standard communication protocol, particularly for aspiring new vendors. New vendors are the next generation that will lead the way once current operatives including myself are retired, arrested, or dead.

Therefore education is a primary key to the ongoing success of the Darknet.

That involves:

1. Manually securing your hardware device.

2. Installing the appropriate system

3. Which software to use

4. Tips and tricks to stay under the radar, even if you are literally talking to the police.

We will write this guide and make it open source in the wiki of /d/opsec after we received donations worth about 250 EUR.

I believe that's fair. /u/HeadJanitor will receive 100% of that money, I will take none. I get my money from vending and my work as a public servant is

in gratitude for everything the community has done for me to support my life.

HeadJanitor, however, is still working full time as a civilian and I believe we should, as a community, come together and help him get out of there and put all his energy into the darknet to build a more beautiful and educated community for all of us.

XMR donation address: 85CShsyZhNt3ViS3CZpdouAvvKkvoAAcnjDbtzkKozUXSRajbwfgWPfdreaXEs1td1LSmBKEjK8fJbfBopbv7m3xDzrSPbG

Please send us a modmail with the XMR transaction ID. Donors will receive a donor flair here in /d/opsec (5 EUR and more).

Once the 250 EUR target was reached, /u/HeadJanitor and I will collaborate this project and publish the guide shortly after.

Yes, I am turning /d/opsec into a public enterprise. That means this will be run as a business. We accept donations, and in return the community wealth grows. You are free to report my endeavors to the hire ups and they can tell me to fuck off if this is wrong. :)

Until then, I'll ***John Galt*** *this community so /u/kaizushi will send me her nudes.*

Note an Ayn Rand Atlas Shrugged reference, yikes!

Thank you very much.

Sincerely,

Pygmalion

4 comments

/u/tito33 OpSec Executioner

I would like to elaborate in writing that guide if you and /u/HeadJanitor are ok with it

/u/Pygmalion Vendor Opsec

Sure, please message us in modmail.

/u/ameeshaposbo

Waiting for the full guide. Hope it will be uploaded soon .

/u/n0stis

"Opsec Guide _for_ Mobile Communication"

This is what is commonly known as an oxymoron or two mutually exclusive terms, not unlike Military Intelligence, or Jumbo Shrimp to paraphrase a George Carlin bit.

calyxinstitute.org is in this business of secure (sic) mobile OS and phones.

Phil Zimmermann (creator of PGP) personally told me that he does not use PGP because it won't work on his iphone and uses Signal instead. OTOH, he is not a Tor user or DM vendor. OTOH he and much of the world seem to be

suffering from "early onset mobile/cloud dementia" in my view. I hereby "coin" this term and its endemic spread across the world and note that this illness primarily impacts the millennial generation. It is truly delusional to believe that you can change a pocket surveillance device or other peoples servers, to provide privacy and anonymity, much less into tools than can be used to your advantage for Dark Web illegal activities.

Then a response from the mod to my previous discussion question regarding DW mail and my posting a link to a white paper on the subject.

Posted on forum and sent in encrypted PM to dread Administrator /u/HugBunter

/u/Pygmalion Vendor Opsec

There really is no point running emails over tor exclusively. Of course you can if you really want to, but it's complicated and inconvenient. Just use PGP and any reliable provider that lets you register anonymously.

There are plenty decent email providers out there. If you think we need another one, go ahead and make one. Squirrel Mail is good frontend software if you wanna go for it imho. That's the one secmail used.

http://sector2nyjrxphgrj3cvnueanomz4trvgyxofvu3cexltoxuegtlmzid.onion/

his one is limited to 10 emails a day but is pretty good, and minimalist.

/u/n0stis

"Of course you can if you really want to, but it's complicated and inconvenient."

That was exactly my point. Go write it yourself is like telling me to screw off. Not a good basis for an OpSec discussion. Are you this arrogant IRL or is this just you posing for the noobs? Or you just like to end discussions on subjects that you were not OP?

Quote: "There really is no point running emails over tor exclusively. "

Response: I think that you should add IMO or IMHO to these statements which are devoid of any factual information. Btw, Squirrel Mail is the front end for Mail2Tor.

/u/Pygmalion Vendor Opsec

Yeah, I've been telling you to fuck off a bunch of times.

Haven't you noticed?

You are annoying as fuck.

"You have been banned from this community.

A moderator at /d/OpSec has banned you until: 14th June, 2032 - 22:31

Reason: Annoying"

/u/n0stis Response: This is really beyond anything that could be considered acceptable behavior from a mod.

To be intimidated by posts that pose reasonable questions and seek discussion (is what forums are about), and it is unconscionable for a mod to disrupt this over a personal vendetta, or being too full of himself to be challenged to support opinions with actual facts.

n0stis

Then 30 minutes later, he got this:

/u/HeadJanitor

You've been unbanned. Please pay no heed to what occurred with him.

This is all true:

Quote: "Phil Zimmermann (creator of PGP) personally told me that he does not use PGP because it won't work on his iphone and uses Signal instead. OTOH, he is not a Tor user or DM vendor."

/u/HeadJanitor Response: Except I heard he's doing better now and has been granted a large fund-award.

https://lwn.net/Articles/880248/

/u/n0stis

Thank you for saving me the trouble of writing this up and bothering you and perhaps paris and hugbunter with this drama. I was considering not doing it at all, which would make for a very different ending for my novel, as five of the dozen or so chapters deal with Tales from the DW, (who and what people are doing there)

Tell me more about Phil's funding, I speak with him on the phone and email occasionally and sent him a photo of Dan Aykroyd doing the BassOmatic thing trying to lure him to be a beta reader for my previous novel. (he liked it a lot but it didn't work). Peace, n0stis

/u/HeadJanitor Moderator

Quote: I am a chamelon. I connect from numerous site-to-site VPNs across the states; all legitimate as a self-assigned guest user of a corporation. I connect from genuine Remote Desktop Sessions on Azure Virtual Networks. I connect from within a datacenter. I run Type 1 Hypervisors and switch operating systems frequently. I connect from business SD-WAN from various industries.

/u/n0stisI Encrypted PM response

Ok, so this description is purposely opaque. But if I can interpret what you don't want to be public knowledge, you use some kind of distributed vpn network to enter various datacenter systems and via Windows RDS virtual sessions to get to the DW. And you take these circuitous routes to maintain anonymity even though you do not visit dark markets. You do this because you see yourself as an LE target due to your mod activities on the DW forums?

/u/HeadJanitor via encrypted PM

Response: Worked like a charm: encrypted again ---->

Response: In brief: I work 10-12 hours a day and use what I have in front of me. Not very elaborate. Haha! I'm a networking guy so this is absolutley nothing special.

n0stis's efforts to stimulate discussions on /d/OpSec were not particularly successful in getting people to write more than a sentence or two (perhaps paranoia about deanonymizing themselves) but it did perhaps stimulate posts like this even though copied verbatim from the Clear Web.

Best Operating Systems for Anonymity: Comparing Titans

by /u/We_Are_9000 Paranoia Level • in /d/OpSec

There are plenty of operating systems aimed at achieving online anonymity. But how many of them are really good? I think that not many. Below I want to suggest several Linux distributions that can help to solve numerous privacy\anonymity issues. https://hackernoon.com/best-operating-systems-for-anonymity-comparing-titans-3501fd5cba3b

Tails OS

Tails is a Debian-based Linux distribution designed to provide privacy and anonymity. All outgoing connections are routed through the Tor network, and all non-anonymous connections are blocked. The system is designed to boot from Live CD or Live USB and leaves no traces on the machine on which it was used. The Tor project is the main sponsor of Tails. This operating system is recommended for use by the Freedom of the Press Foundation and was also used by Edward Snowden to expose PRISM.

In order to evaluate all the pros and cons of Tails, it is necessary to have a strong understanding what purposes this OS was created for and how it should be used.

This operating system can launch very quickly. After creating a flash drive, it will take 1–2 minutes to access the Internet (in case you have good hardware). However, you should not expect much functionality from Tails. It allows you to quickly connect to the Tor network, use messengers and connect via a secure channel, generate and save passwords, and clear metadata files.

At the heart of Tails lies the task of ensuring the anonymity and safety of the user on the network, while at the same time preserving the convenience and ease of use. And it does it quite well. The whole system works in Live mode uploaded into RAM. Tails is not installed onto SSD or HDD. After the session is over, it is impossible to determine what the user was doing on the computer, even if somebody will get full access to the device.

This OS is not recommended to be used as a permanent operating system. After shutting down or restarting the system, all downloaded files, browser history, etc.—are deleted.

You can create a Persistent encrypted partition and store passwords and files of various types on it, but these files should be not very sensitive.

To run Tails, you need a device with at least 1GB of RAM and an antediluvian processor. Optimal device specifications for Tails: 8GB RAM and a 2-core processor.

Installation of third-party programs is not the strong side of this OS. Installing applications onto Tails is not the most pleasant thing. There are often unforeseen errors, even if everything is done correctly. It may happen that after several reboots your installed software may simply disappear. If you need to systematically work with third-party software, the best option is to create your own distribution that will fit your needs.

The goal of Tails is to leave no traces, anything more than accessing the Tor network and storing files can be a problem. It is best to use Tails for getting quick access to the network, connecting to a remote web resource, working with documents, communicating over an encrypted channel, sending\receiving cryptocurrencies.

Tails pros:

- *Quick access to the network (Tor, instant messengers, online crypto-wallets).*
- *Built-in tool for cleaning metadata.*
- *Built-in instant messengers.*
- *Generation/storage of passwords.*
- *Works with almost any hardware.*

Tails cons:

- *Difficult installation.*
- *Problems with the installation of third-party software.*
- *Not suitable as a permanent OS.*
- *Not suitable for storing highly sensitive\private files.*

Tails is a good system. It has its drawbacks, but again, it is simply tailored to specific tasks that do not always work for all users. Tails is more concerned with the issue of anonymity, but not security. Of course, this is an anonymous and quite good secure system, but there are other distributions that are much more advanced. Tails is well-known thanks to Snowden and gets advertised by many communities due to its simplicity.

Whonix

Whonix is a Debian-based Linux distribution, formerly known as TorBOX. Designed to ensure anonymity by means of VirtualBox and Tor. Neither malware nor compromised superuser account can lead to IP and DNS leaks. All software bundled with this OS is pre-configured to work with maximum security settings.

Whonix OS consists of two virtual machines: Whonix Gateway and Whonix Workstation, connected through an isolated network. Gateway works

exclusively through Tor and acts as a gateway to the network, Workstation works in a completely isolated network.

All network connections are possible only via Tor. The only network access for the workstation is the gateway. All traffic, all applications, and processes will go through Tor.

Applications cannot access the Internet bypassing Tor. Applications can only see the local IP address. The time zone cannot be traced, the clock is set to UTC, and Timestamp HTTP headers get sent to randomly selected web servers.

The possibility to implement different sequences of Tor + VPN is a great advantage of this OS. You can configure the system so that first all the traffic goes through the VPN, after that through Tor, and then again through the VPN.

Whonix is a system with wide possibilities of customization and configuration that sometimes cannot be done in Tails. There are many programs and settings that allow you to build your own anonymity/security system, remove traces of using files, use instant messengers, work with different file types, etc.

Whonix is definitely a good system for anonymous Internet access but using it on an ongoing basis will be quite problematic. Since Whonix is built around virtualization, this may cause some problems. For example, you can face difficulties while working with external media. If you need to connect a USB flash drive, it will first go through the main OS, for example, Windows, then go through the VirtualBox and finally reach the Whonix system, and this is not the safest way.

Whonix pros:

- *High degree of anonymity.*
- *A large number of software tools to work with.*
- *Wide fine-tuning possibilities.*

Whonix cons:

- *Not portable.*
- *Requires powerful hardware.*
- *Tied to VirtualBox, which brings big risks in case of hacking the OS on which VirtualBox is installed.*
- *Not quick, requires more time to access the network than other operating systems (you need to start VirtualBox, Gateway, Workstation).*

Whonix is good as a secondary (additional) system because it is not portable. Portability is one of the most important criteria in this segment. It is also tied to VirtualBox, and since this is not a live system, it will be quite easy to detect the presence of Whonix if you do not use cryptography methods.

Whonix should be used only in special cases. I put it on my list because it is very flexible in terms of settings.

Kodachi

Linux Kodachi is based on Debian too. The goal of Kodachi is to provide the most anonymous and secure access to the network and protect the system itself. All traffic is running through a VPN, then through the Tor network with DNS encryption. Free VPN is already pre-configured.

Kodachi is positioned as an anti-forensic OS that makes forensic analysis of drives and RAM really difficult.

XFCE was chosen as the desktop environment for Kodachi, the system design is very similar to MacOS. System and network parameters are shown in real time on the desktop, which allows you to monitor the system and also monitor the operation of the Tor and VPN networks.

Kodachi supports DNScrypt, a protocol, and utility that encrypts requests to OpenDNS servers using elliptical cryptography. It eliminates a number of typical problems, such as DNS leaks and leaving traces of network activity on the provider's servers.

If you need to hide an IP address in P2P networks, you can use PeerGuardian. If you need to work with suspicious processes, they can be easily isolated using the built-in sandbox called Firejail. A nice option is the ability to quickly change the Tor exit nodes with the option to select a specific country using Multi Tor. Kodachi has a decent amount of pre-installed software for solving any tasks, for example, to encrypt information (VeraCrypt, TrueCrypt), to send confidential messages (GnuPG, Seahorse, Enigmail, GNU Privacy Guard Assistant) for hiding traces (MAT, Nautilus-wipe, Nepomuk Cleaner, BleachBit).

In addition, Kodachi has its own browser based on the Tor Browser, where its developers cut out some problematic Tor modules.

Kodachi is a well-balanced system, it is a powerful tool for building anonymity and security systems in all understandings. This OS is best used in conjunction with encrypted media on which highly sensitive information can be stored.

In my opinion, Kodachi is the best system at the moment, it allows you to solve plenty of tasks.

Kodachi pros:

- *Quick start (i.e. fast network access like Tails).*
- *Many pre-installed programs.*
- *Not very demanding in terms of hardware.*

There are actually no cons but they may appear with some narrowly focused tasks \ needs.

There are some other quite good operating systems built for anonymity such as Subgraph and Qubes.

Qubes

Qubes OS uses an interesting principle to launch applications. Each app runs on a separate virtual machine. Apps are divided into classes depending on the level of importance. The browser runs on one virtual machine, the messenger runs on the other virtual machine. For the user, both programs seem to be running on the same workspace. Isolating applications means that if malware gets inside, personal files will not be compromised.

Qubes OS works only after installation on the internal drive, it does not have a live mode.

Subgraph

The key idea behind Subgraph OS is running custom applications on isolated sandboxes. To do this, the subsystem Oz is used. Oz consists of a daemon (system service) that receives requests to create sandboxes, an Xpra X-server, and a set of special utilities.

Subgraph OS is a bit raw tool. Only the alpha version is available right now.

Subgraph and Qubes are not bad, but they are not good enough to put them among leaders. Subgraph OS is too raw, Qubes is too confusing in terms of settings.

2 comments

/u/BabyLordaSosa

Very good thread, well detailed and well summarized.

/u/hashseekerus

Kodachi is an immediate no-no for me because it includes a VPN. VPN -> Tor is known to be a security flaw.

Despite his reluctance, n0stis, aka arister0s on the Hub, decided to post three OpSec questions on Mixnets, dVPNs, and Tor email clients in the Security forum of the Hub and found this:

The Hub - Info Center

Users Online

1 Guest, 3 Users

Users active in past 60 minutes:

arister0s, mikmik987, breadbin595595

Most Online Today: 5. Most Online Ever: 1574 (June 28, 2019)

So apparently not a real popular place these days. With all the sniping and snark aimed at noobs, it is no wonder.

And OH Shit I have to do the 20 posts thing again, with the quadruple CAPTCHA, this time as arister0s. Is it worth the effort?

So arister0s posted 20 messages with famous quotes to yet again complete this initiation ritual including this one:

"When the going gets weird, the weird get going."
Hunter S. Thompson

arister0s did get a response on the Hub.

FatherTed

- *Vendor*
- *Legendary Contributor*
- *Posts: 2016*
- *Community Rating: +410/-485*

Re: Is anyone using a Mixnet?

« Reply #1

- *Quote*

Never heard of it before, But that's whats great about questions. Thanks for something for me to read into, +1

Those whom dwell in the house of elliptic curves shall forever be encrypted for all time, Amen.

arister0s

- *New Contributor*
- *Posts: 24*
- *Community Rating: +1/-1*

Re: Is anyone using a Mixnet?

« Reply #2

Not as well received over on /d/OpSec

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/4458463e4ca3c468da5a

FatherTed

- *Vendor*
- *Legendary Contributor*
- *Posts: 2017*
- *Community Rating: +410/-485*

Re: Is anyone using a Mixnet?

« Reply #3

- *Quote*

Well, I've done some reading into it, and to be honest I can't see myself ever using it nor can I see it ever becoming something mainstream users would bother using either.

Tor already hides metadata, And using PGP to send messages is already a

strong enough encryption. You seem to know more about this than I do, So please tell me what are the benefits of using this? Like what purpose would it serve to you or me that can't be done with what I already use?

Those whom dwell in the house of elliptic curves shall forever be encrypted for all time, Amen.

arister0s

- *New Contributor*
- *Posts: 25*
- *Community Rating: +1/-1*

Re: Is anyone using a Mixnet?

« Reply #4 on:

"Tor already hides metadata..."

Response: Quoting from the whitepaper:

"The core component of Nym is a mixnet that protects network traffic metadata for applications, providing communication privacy superior to both VPNs and Tor against global adversaries that can watch the entire internet. Even though Tor protects metadata much better than VPNs, it is designed to do so only against network adversaries who have limited ability to monitor the entire network. Network adversaries that observe both the traffic incoming and outgoing from Tor can perform end-to-end correlation attacks and de anonymize the connection."

arister0s In my view it is about mixing, introducing dummy packets, and disrupting timing.

To FatherTed Via encrypted Hub PM

I would like to talk more about this via email perhaps?

n0stis@mail2tor.com

arister0s (aka n0stis)

FatherTed

Vendor

Legendary Contributor

Posts: 2018

Community Rating: +410/-485

Re: Is anyone using a Mixnet?

Quote

To be honest with you, I think this is nothing but Vaporware. It has zero financial backing from the privacy research community. Nym is just another way to sell useless tokens. Similar networks like this include :

Orchid Protocol, Mainframe, Obsidian, Skrumble, Dusk.

None of them including mixnet are without blockchain/payment as a component. Its useless nonsense, It won't compete with Tor because of its laughably small Network. Sure it might sound great on paper, But that is

where it ends. If you are considering investing into this, I'd avoid it.

Those whom dwell in the house of elliptic curves shall forever be encrypted for all time, Amen.
SR1 - BMR - SR2 - Utopia - Agora - Sheep - Evolution - Abraxas - Traderoute - MiddleEarth - Hansa - Alphabay - Dream - WSM

Hungry_Eyes

New Contributor

Posts: 44

Community Rating: +4/-1

Re: Is anyone using a Mixnet?

« Reply #6

Quote from: FatherTed

"To be honest with you, I think this is nothing but Vaporware. It has zero financial backing from the privacy research community. Nym is just another way to sell useless tokens. "

I had the same feelings when I saw this on Dread a week or so ago. Sounds good in principle, but not terribly practical at this time.

benihana

Full Contributor

Posts: 174

Community Rating: +438/-232

reformed troll

Re: Is anyone using a Mixnet?

« Reply #7

Quote

Just put all that work in more Tor exit nodes and the "possibility to track the entire network" becomes smaller

arister0s

New Contributor

Posts: 26

Community Rating: +1/-1

Re: Is anyone using a Mixnet?

« Reply #8

Quote: "None of them including mixnet are without blockchain/payment as a component."

Response: Since Tor is a volunteer unfunded system, systems are routinely down, server, network hardware and bandwidth are weak. Geographical diversity is also a problem with almost 40% of the 7500 or so Tor nodes being in the US or Germany.

Tokens (payment) are a way to build a more professional system.

I noticed you didn't respond to my point about metadata.

Funding is primarily from venture capitalists like most other startups.

Nym Technology Secures $13M Funding Led by Andreessen Horowitz

www.coinspeaker.com/nym-technology-13m-funding/ 2021-11-18

However, this is not the first funding raised by Nym Technology. Back in 2019, Nym raised $2.5 million in seed investment led by Binance's VC arm. Also, earlier this year in July, Nym raised $6 ...

Nym Raises 6.5 million USD in VC Funding | by Nym | nymtech

blog.nymtech.net/nym-raises-6-5-million-usd-in-vc-funding-2021-07-19

Neuchâtel, Switzerland, July 19th, 2021. As recently reported in TechCrunch, European privacy startup Nym Technologies has received a 6.5 million USD (5.5. million EUR) round of funding from venture capital in order to build an open source and decentralised privacy network that plans to compete against closed source privacy networks such as ...

Privacy Startup Nym Raises $13 Million in Third Funding Round Led by a16z

cryptopotato.com/privacy-startup-nym-raises-13-million-in-third-funding-round-led-by-a16z/ 2021-11-18

a16z and Others Invest In Nym. According to an official press release shared with CryptoPotato, the just-concluded investment round was led by the leasing Silicon Valley firm - Andreessen Horowitz (a16z). Nym noted that the fresh cash injection will be used to expand its community and add a dedicated project team just before the launch of its ...

FatherTed

- *Vendor*
- *Legendary Contributor*
- *Posts: 2027*
- *Community Rating: +411/-485*

Re: Is anyone using a Mixnet?

« Reply #9

- *Quote*

What point did you make? I don't think you know your head from your ass to be honest. Go and waste your money on this bullshit and the rest of us will carry on as we are

Tor Browser was made by the US military, And is funded by the US military. Though it does accept voluntary donations. Also, Its free for everyone to use unlike this crap.

If you want to carry on trying to convince me or anyone here about this, Try to actually use your brain and not copy and paste stuff from elsewhere. Nobody on Tor cares about this as we already have a working system, And if it ain't broke then why try to fix it.

Besides, WTF do you intend on doing that you would even require such so called "best" security? After all most of these setups are usually made so the ISP or government doesn't know what you are doing so what is it you personally want a mix net for that can't be done using a free service like Tor??

When I get up to no good I just hack an internet connection, Just like I am using now.

Those whom dwell in the house of elliptic curves shall forever be encrypted for all time, Amen.
SR1 - BMR - SR2 - Utopia - Agora - Sheep - Evolution - Abraxas - Traderoute - MiddleEarth - Hansa - Alphabay - Dream - WSM

FatherTed

- *Vendor*
- *Legendary Contributor*
- *Posts: 2027*
- *Community Rating: +411/-485*

Re: Is anyone using a Mixnet?

« Reply #10

- *Quote*

Quote from: Hungry_Eyes

I had the same feelings when I saw this on Dread a week or so ago. Sounds good in principle, but not terribly practical at this time.

I will entertain his question until he gives me some decent insight, But from what I can gather its just to get people investing in there coin. I don't see a working version of it anywhere so as of now its all talk and no action

Those whom dwell in the house of elliptic curves shall forever be encrypted for all time, Amen.
SR1 - BMR - SR2 - Utopia - Agora - Sheep - Evolution - Abraxas - Traderoute - MiddleEarth - Hansa - Alphabay - Dream - WSM

ImproveHousingBathroom

- *Jr. Contributor*
- *Posts: 74*
- *Community Rating: +10/-7*

Re: Is anyone using a Mixnet?

« Reply #11

Quote

uses blockchain technology to mix and scramble packets of metadata

Blockchains are a way to have an immutable permanent record of things. An immutable permanent record is the last thing you'd want for your secret network activity.

Quote

network layer 0

There is no such thing.

Quote

reordering the messages they route TCP doesn't necessarily like when its packets get reordered too much.

Quote

untraceable ... as well as timing

Sounds slow. And it relies on assuming that traffic analysis tools are a lot more fragile than I think they actually are.

arister0s

- *New Contributor*
- *Posts: 28*
- *Community Rating: +1/-1*

Re: Is anyone using a Mixnet?

« Reply #12

Ah, you have much to learn grasshopper.

https://www.belden.com/blogs/osi-seven-layer-model-where-does-layer-0-fit

https://orhanergun.net/what-is-layer-0-in-the-osi-layers/

hamfistedbimbo

- *Full Contributor*
- *Posts: 222*
- *Community Rating: +11/-90*

Re: Is anyone using a Mixnet?

« Reply #13

- *Quote*

Tor is a mixnet, we're all using one silly

reinstated after being unjustifiably banned for an obivous joke.
To the admin who reinstated me: thx.
to the admin who banned me: tight ass for a faggot. lighten up u little bitch

arister0s

- *New Contributor*
- *Posts: 28*
- *Community Rating: +1/-1*

Re: Is anyone using a Mixnet?

« Reply #14

I guess for those who are not willing or able to read the whitepaper in the link I posted, an intelligent conversation will not occur. It does address questions posed here.

Unless you are willing to consider and respond to the question I posed regarding metadata capture by someone who can see entry and exit points (NSA tools were hacked) then an intelligent conversation will not occur.

If you want to ignore and diminish the clear evidence of venture capital

investments being made an intelligent conversation will not occur.
Quote from: FatherTed
Quote from: Hungry_Eyes
I had the same feelings when I saw this on Dread a week or so ago. Sounds good in principle, but not terribly practical at this time.
I will entertain his question until he gives me some decent insight, But from what I can gather its just to get people investing in there coin. I don't see a working version of it anywhere so as of now its all talk and no action
arister0s

- *New Contributor*
- *Posts: 28*
- *Community Rating: +1/-1*

Re: Is anyone using a Mixnet?
« Reply #15
Not hard to find. Download the latest version of Nym software for your operating system.
MacOS 11 Big Sur, 12 Monterey x86-64, Ubuntu 20.04 x86-64, Windows 8.1, 10 and 11 x86-64
View the source code on GitHub. See the changelog for a full list of changes.
https://nymtech.net/download/

Now a normal person's reaction to something not in his or her knowledge base would be skepticism, followed perhaps by curiosity, followed by some quick research. On the DW however, in general, denial seems to be the natural reaction followed by attacking the messenger when facts show otherwise, and conflicts with preconceived beliefs, superstitions, or rituals.

arister0s believed that one of the keys to his success in 35 years in the IT field was his lifetime insatiable curiosity about all thing tech. To him the demonstrated incuriosity seemed to be in direct conflict with operational security.

FatherTed
Vendor
Legendary Contributor
Posts: 2035
Community Rating: +411/-485
Re: Is anyone using a Mixnet?
« Reply #18
Quote

"I don't see a working version of it anywhere so as of now its all talk and no action"

You think that me, Is LE? :D

Why don't you remove your head from your ass like I said earlier and read about where and who you are preaching to. We are all a mixture of drug dealers, Fraudsters, Hackers and recreational drug consumers both here and on Dread. Nobody gives a single fuck about this "mixnet" as it doesn't allow or serve to any of the reasons we use the darknet.

How can one have an "intelligent" conversation on something they don't know about nor want to know about?

You don't seem to have any understanding of why people use Tor, The vast majority of users are here for nefarious reasons. And these nefarious sites are not hosted on mixnets nor can they be hosted on mixnets, The only place they exist is on Tor and I2P.

So I advise you go and find a clearnet forums to chat about this topic, Because as you can see here and on dread. Nobody gives a shit ::)

Those whom dwell in the house of elliptic curves shall forever be encrypted for all time, Amen.
SR1 - BMR - SR2 - Utopia - Agora - Sheep - Evolution - Abraxas - Traderoute - MiddleEarth - Hansa - Alphabay - Dream - WSM

Hungry_Eyes

Jr. Contributor

Posts: 58

Community Rating: +7/-1

Re: Is anyone using a Mixnet?

« Reply #19

Quote from: FatherTed

Quote from: arister0s

"I don't see a working version of it anywhere so as of now its all talk and no action"

Not hard to find. Download the latest version of Nym software for your operating system. MacOS 11 Big Sur, 12 Monterey x86-64, Ubuntu 20.04 x86-64, Windows 8.1, 10 and 11 x86-64

You think that me, Is LE? :D

Halleluyah! Father Ted a preachin' the Gospel! +1

jjiolo

- *Jr. Contributor*
- *Posts: 61*
- *Community Rating: +6/-4*

Re: Is anyone using a Mixnet?

« Reply #20

- *Quote*

tor's a bit naff[52] against an attacker with a full network view*. you can sit on every node in the network and correlate traffic into and out of it by matching packet order and size same way an isp can fully correlate vpn traffic.*

mix nets buffer input and randomize the output and size. pretty much the only viable way to make a proxy network against an attacker with a full network view that doesnt require hopping multiple countries in the hopes of gaining obscurity.

works well as a roll your own halp im being oppressed kit.

nym on the other hand looks like a total scam.

thought most of you dinosaurs would have known more about email mix nets and where most of this stuff started from.

FatherTed

- *Vendor*
- *Legendary Contributor*
- *Posts: 2035*
- *Community Rating: +411/-485*

Re: Is anyone using a Mixnet?

« Reply #21 on: Today at 03:41:59 PM »

- *Quote*

Quote from: jjiolo

thought most of you dinosaurs would have known more about email mix nets and where most of this stuff started from.

Honestly I personally never really looked into it. *I know about proxychains and from what I can gather this is just a more secure form of that but with a payment wall around it.*

Those whom dwell in the house of elliptic curves shall forever be encrypted for all time, Amen.

arister0s

- *New Contributor*
- *Posts: 35*
- *Community Rating: +1/-2*

Re: Is anyone using a Mixnet?

« Reply #22

Quote from: FatherTed

Quote from: arister0s

“How can one have an "intelligent" conversation on something they don't know about nor want to know about?”

---

[52] naff is British slang, meaning uncool, tacky, unfashionable, worthless...

I guess to me an intelligent conversion means the absence of name calling and swearing, exchange of facts, and no acknowledgement that you are just a bad person and your bad behavior is thus excused. " We are all a mixture of drug dealers, Fraudsters, Hackers and recreational drug consumers"

Remember, I simply asked a question if anyone is using a mixnet and I wanted to know why or why not. Facts not opinions.

I never advocated for mixnets, never talked about investing or encouraged anyone to invest, despite be accused of this. I believe that it is clear who posts facts and who is reacting out of come preconceived notions, biases, prejudices, or fear of something new.

If you both explain that you know nothing about it and also offer an opinion, I take that as BS.

Nobody on the DW cares about OpSec? Is that the drugs talking now?

jjiolo

Jr. Contributor

Posts: 61

Community Rating: +6/-4

Re: Is anyone using a Mixnet?

« Reply #20

Quote

thought most of you dinosaurs would have known more about email mix nets and where most of this stuff started from.

FatherTed

Vendor

Legendary Contributor

Posts: 2035

Community Rating: +411/-485

View Profile Personal Message (Offline)

Re: Is anyone using a Mixnet?

« Reply #21

Quote

Quote from: jjiolo

thought most of you dinosaurs would have known more about email mix nets and where most of this stuff started from.

FatherTed response

Honestly I personally never really looked into it. I know about proxychains and from what I can gather this is just a more secure form of that but with a payment wall around it.

Ok, so he never really looked into mixnets, never looked at the whitepaper I offered, but yet was abusive and condescending to arister0s but not to jjiolo because of his being a noob or just because he needed to live up to his description of himself and his peeps.

arister0s
- *New Contributor*
- *Posts: 26*
- *Community Rating: +1/-1*

Anyone using decentralized VPN's?
What about decentralized VPN's (dVPN) such as Orchid or Sentinel?
Too complicated?
Too untested?
Too expensive?
Never heard of them?
benihana
- *Full Contributor*
- *Posts: 174*
- *Community Rating: +438/-232*
- *reformed troll*

Re: Anyone using decentralized VPN's?
« Reply #1
- *Quote*

I'm using bridges

Then with regard to the Tor web mail question:

arister0s
DW email and OpSec
What if you could Keep the NSA Out of Your Inbox? Anyone monitoring the email would be able to see the size of the message but that's about it. If sent over a Mixnet, not even that will be seen.
https://darkmail.info/downloads/dark-internet-mail-environment-march-2015.pdf
Thoughts?
benihana
Full Contributor
Posts: 174
Community Rating: +438/-232

reformed troll
Re: DW email and OpSec
« Reply
Quote
I think I'm not downloading a pdf file
The client sounds interesting
arister0s
New Contributor
Posts: 27
Community Rating: +1/-1
Re: DW email and OpSec
« Reply #2
So your OpSec is that you never download a pdf from the clear web?
You must lead a boring life.

Insider Story Four </html>

A Secure Privacy Web skipping Web 3 for Web 4 and beyond

The web was designed to bring people together and make knowledge freely available. It has changed the world for good and improved the lives of billions. Yet, many people are still unable to access its benefits and, for others, the current Web comes with too many unacceptable costs.
Contract for the Web https://contractfortheweb.org/

Web 1-a static web of links to documents

Web 2- dynamic web with walled gardens of social media, corporate data harvesting, privacy theft, dystopian realities, and invasive advertising

Web 3- coined by Gavin Wood speculative, crypto/blockchain, identity free, cutting the Big Tech middlemen out by decentralizing the web in the way cryptocurrency is wresting control of world finance from institutions and governments. Uses excessive resource intensive mining and speculation. Most likely venture capitalists will replace the likes of Google and Facebook as the autocrats of Web3.

Web 4 –what we are attempting to build now

- **Forth Goal: We will use a Mixnet, modeled after Nym[53], but will be public rather than private, to secure network level privacy. This network will protect even against the most powerful, passive adversaries that can observe every packet going in and out of your Internet connection. It will be engineered so that you can be online anytime and anywhere without the fear of being watched. This infrastructure will prevent any data leakage by protecting every packet's metadata at both the network and application layers.**

[53] *The Nym network ("Nym") is a decentralized and incentivized infrastructure to provision privacy to a broad range of message-based applications and services. The core component of Nym is a Mixnet that protects network traffic metadata for applications, providing communication privacy superior to both VPNs and Tor against global adversaries that can watch the entire Internet comings and goings.*

Our Manifesto

We are a group of people who are attempting to spearhead the redesign of the entire Internet. We will put the power in the hands of the people, rather than major corporations, it will be an egalitarian web where you and I, and not Big Tech like Google and Facebook, have control over our own online presences, finances, and data. These are the basic concepts.

Some believe the individualization of all web users provided by Web3's ideals could balloon all of these malicious activities and spawn entirely new ones. The reason for this fear is the utterly anonymous nature of Web3's underlying infrastructure. Just as cryptocurrency has been used to support criminal activity by providing an anonymized method of payment that's beholden to no government or bank, so Web3's tokenized system could also help criminals remain untraceable by any governmental or law enforcement authorities.

Of course, as with any tool, it is all about the people that use it. Citizens living under repressive regimes could benefit greatly from the type of anonymity that could also enable any of the aforementioned crimes.

Web 4 will not have any in-place cryptographic ledger to draw from. An alternative method of handling tokenization will be found.

There will be no NFTs, which are the digital equivalent of a banana duct-taped to a wall: something literally anyone can own at little or no cost, yet they now want you to pay for this idea of its ownership. This in a world where celebrities are coughing up more than half a million dollars for a jpeg of a cartoon ape, it is clear that the sector has been overrun by greed, or perhaps being used as a vehicle for money laundering schemes.

All online security relies on one very fallible factor: human beings. They could potentially expose themselves to identity theft and fraud just as easily as they can today. If they hand over one of those cryptographic keys, it would be no different, and possibly even worse, than if they divulged a credit card or social security number.

New methods of verification and authorization will be devised to combat scenarios like this.

Web4 will not be the Internet trading one set of overlords for another. Venture (vulture) capitalists and their Limited Partnerships LPs, will not replace the likes of Google and Facebook as the autocrats of the web. People will. A globally diverse collective of individuals, coming together in a new area of cyberspace that allows each user to be their CEO. On this new web, you will control your own data, profit (or not) from the sale of all of your information, and remain secure behind tokenization.

We will change basic and fundamental structure of the entire Internet ecosystem.

This type of a true sea change will come but it will not be fast, and it may not exactly resemble what we envision right now, given the unpredictable nature of humans.

Options

In helping to lead the web to its full potential, a number of options were considered for the group to support including:

One option is for the government to nationalize telecommunications infrastructure. It having mostly been paid for by the public anyway, and obviously not working on behalf of the public now to the tune of the four hundred billion dollar broadband scandal. No more throwing good money after bad was one thought.

Other options include a new agency a Public Service Communications Commission, the repeal of state laws banning broadband competition, and the implementation of a plan for permanent net neutrality. That would mean that there would be no intentional fast lanes and slow lanes for data, which are now being created based on financial profit considerations.

There could be no Internet routers trying to peek at packet content to vary their delivery behavior accordingly. This is not innocuous packet header inspection, which determines the destination, but rather deep packet inspection routing and forwarding algorithms, or DPI. This practice is incompatible with privacy, anonymity, and network neutrality. The current weak specification, which is silent on what the network should not do, opens the door to the malicious behavior we see on the Internet today. Encryption of the packet contents inside the Mixnet thwarts this behavior.

Access and cost

It should by now known to all that Internet access has become one of freedom's material preconditions. It is one of the resources that people need in order to rule themselves in a democracy. A system that allocates this resource solely according to the logic of profit is incapable of providing it to everyone as a matter of right. If profit is the principle that determines how connectivity is distributed, millions will be forced to go without it. Those who cannot afford to pay, or those who live in places that are not profitable enough to invest in are in a Digital Divide. Many more will have only a precarious grasp on it, contingent on the size and regularity of their paychecks. Those who can afford the extortionate fees of the broadband cartel will endure the abysmal speeds and service resultant of chronic underinvestment of those seeking to maximize shareholder investment rather than serve their primary customers.

Alternately, there are publicly owned electric distribution utilities building smart grids. These can be funded by bond issues or federal stimulus grants, with the idea of making the grid more efficient by embedding sensors and other digital devices that monitor the system in real time. Problems could be detected early, which would help reduce outages and improve reliability. The smart grid can also provide the infrastructure to become an Internet Service Provider or ISP. The smart grid running on a fiber-optic network, allows the monitoring devices to communicate, and can run all the way to people's homes as FTH or fiber to the home.

These ISP's can be operated by rural electric or telephone cooperatives, owned, and controlled by their members, and users of their services.

Data Protections and Interoperability

Beyond access and service, we need to solve the data collection, privacy invasion problem. Google remains the apex predator of data theft followed by Facebook, Microsoft, and Apple with their black boxes inside of black boxes inside of black boxes. Billionaires known as Jeff and Mark have become the moral and gender neutral Typhoid Mary's of surveillance capitalism in what can only be described as a Teflon industry, free of any reasonable regulations.

Efforts will also need to be made to resolve the massive inequity problems in the US. As the economy has slowed down, it has also become more unequal. Since the 1970s, the richest .01 percent of Americans have more than quintupled their share of the country's total wealth.

Many believe that monopolies posed a threat to democracy, and that a system of checks and balances is required to disperse corporate power and promote fair competition.

Instead of one Facebook, imagine thousands or millions of social media communities, webs of application streaming audio and video services each with their own rules and customs and cultures. These communities would host different kinds of interactions, as do our current pool halls, libraries, and churches. In common, they are all public spaces, with different purposes, norms, and diversity.

Decentralization facilitates greater diversity but also enables a degree of active democracy. These new social media and streaming communities can become self-governing making their own choices, guided by considerations other than profit. Themselves no longer being forced to let tech executives decide how filtering algorithms work or how content is moderated, behind closed doors and bound by the market.

Just because such communities would be small does not mean they would have to be isolated. Decentralization is not fragmentation. The Internet is currently made up of many distinct networks, and our data travels easily across them because the networks share a common set of protocols. These protocols all need to be open and nonproprietary so that any network can join as long as it follows the specified rules.

Interoperability means that the advantages of network effects can be preserved without the network being owned by any single entity as demonstrated by email. Gmail and Yahoo Mail are distinct services with distinct features, yet users can still exchange messages due to shared protocols.

Returning to the roots of an open Internet

The fact that Internet protocols are open and nonproprietary is a direct consequence of the internet's public origins. Privatization has now pushed things in the opposite direction with online life increasingly takes place within monolithic enclosures where interactions are governed by secret and proprietary algorithms. "Protocolizing" social media and streaming audio and video applications for example, could break the walls of these walled gardens.

Imagine a technical concept sometimes called "adversarial interoperability," where one Internet service communicates with another without the latter's permission, or with grudging permission secured through legislation. Facebook, YouTube, and other monopolies could be made to adopt open protocols that enable other media applications to interconnect. This interaction would be based on socially useful production and not profit.

Creating these new networks that will need to start small and become more robust, will require public investment.

Each one could have a federated social media and streaming server, and anybody with a library card could have an account. Using existing public infrastructure is an excellent way to make new online spaces more accessible, and fasten them to a funding source, while adding a measure of accountability. Libraries have a further advantage: they are full of librarians who are the original information workers. Their job is to retrieve, classify, curate, and contextualize information as a public service, which is needed in online spaces.

An applicable excerpt from my 2014 book The Insider (A Life Inside the Personal Computer)

In addition to wring the classrooms for networking, and providing computer systems for each classroom, they sought to give these kids access to the outside world. Due to the high cost and limited availability of high-speed Internet connections at the time in 1995, Lefty and his nonprofit volunteer team also built the elementary school an Internet web proxy server connecting to a donated dial-up phone connection from a local Internet Service Provider or ISP. He placed the server, installed with web page archiving software, inside the library for the librarian to download, and curate age appropriate educational Internet website content. The teachers would then call the web pages up over the local area network or LAN, bringing this content into the classroom for the kids to access to these learning curricula.

References:
Tarnoff, Ben. Internet for the People, Verso
Clark, David D. Designing an Internet (Information Policy) MIT Press.

"Back to the task of destroying Facebook.
Or could be design and implement an EMP attack?"

An electromagnetic pulse (EMP), also a transient electromagnetic disturbance (TED), is a brief burst of electromagnetic energy. Depending upon the source, the origin of an EMP can be natural or artificial, and can occur as an electromagnetic field, as an electric field, as a magnetic field, or as a conducted electric current. The electromagnetic interference caused by an EMP disrupts communications and damages electronic equipment;

https://www.startpage.com/do/dsearch?query=emp+attacks&cat=web&pl=ext-ff&language=english&extVersion=1.3.0

Hacker downloaded a cracked version of Ansys HFSS (high-frequency structure simulator), is a commercial finite element method solver for electromagnetic (EM) structures. Ansys HFSS is a commercial finite element method solver for electromagnetic (EM) structures from Ansys that offers multiple state-of-the-art solver technologies. Each solver in ANSYS HFSS is an automated solution processor for which the user dictates the geometry, properties of the material and the required range of solution frequencies.

Hacker downloaded a cracked version of Ansoft Designer a highly accurate design flow that allows users to precisely model and simulate complex analog, RF, and mixed-signal applications and perform signal-integrity analysis and system verification of high-performance IC/package/board designs. This flexible, easy-to-use software includes schematic and layout capture, netlist generation, a planar electromagnetic solver (Method of Moments), and sophisticated data visualization and analysis tools."

With Facebook now destroyed, we could focus on building Web 4.

To be continued…

Part Five: A Place Online Without Identity

http://www.the_insider_goes_deep/tales5.html

So /u/n0stis sent an improved DW Hosting document in an encrypted dread message to a couple of dread mods /u/matter and /u/Cyberjagu.

I have updated the /u/matter original list, removed duplicates and introduced some formatting. Please review for errors, and you may use the finished product and post on a sub like /hardware or for info for newbies.

The document was posted at this site:

https://anonfiles.com/D03aMdZdxb/DW_Hosting_pgp

-----BEGIN PGP MESSAGE-----

Version: BCPG v1.63

~~*ENCRYPTED MESSAGE*~~

-----END PGP MESSAGE-----

And then the response:

Quote: >I have updated the /u/matter original list, removed duplicates and introduced some formatting. Please review for errors, and you may use the finished product and post on a sub like /hardware or for info for newbies.

>The document is posted at this site:

>https://anonfiles.com/D03aMdZdxb/DW_Hosting_pgp

Response: thank you very much but why did you do this?

Quote: " thank you very much but why did you do this?"

Response: Because you were helpful to me when I asked, and to contribute

something to the greater good of the DW privacy goals. To not just be a taker.
Also, I am a writer doing research for a historical novel about the Dark Web. I am not a journalist, but I am looking to have discussions with a number of people on a number of topics on dread, The Hub, Raddle and maybe Envoy.
I think that you as a dread mod would be a good choice for me if you are willing. I am not looking to expose anything other than get some ideas of who and why people are here and what they are doing. Am interested in legal activities only. n0stis
-----BEGIN PGP MESSAGE-----
Version: BCPG v1.63
~~ENCRYPTED MESSAGE~~
-----END PGP MESSAGE-----

And the response? All of the following encrypted message means:

-----BEGIN PGP MESSAGE-----
~~ENCRYPTED MESSAGE~~
-----END PGP MESSAGE-----

This:
no time sorry. Good luck
And then my response:
Well that is exactly why I did not bug /u/paris or /u/hugbunter.
This might be a silly newbie question, but does dread have a PR person?

-----BEGIN PGP MESSAGE-----
Version: BCPG v1.63
~~ENCRYPTED MESSAGE~~
-----END PGP MESSAGE-----
Response to a personal message to
BenzoBore
Jr. Contributor
Posts: 70 (1.186 per day)
Personal Text: Фёдор Михайлович Достоевский
Community Rating: +12/-0
Reply: I cannot be of much help to you with writing as I am not much help to myself, given my own occupation especially. If you want the Dark Web to help you, you've got to help the Dark Web.

-----BEGIN PGP MESSAGE-----

hQEOA+iIt1NQ+KmHEAP/daKaNLujIL4o1ApUEOg+RGSYkCDFe8IUJW
HrDi+7DZ+C
8XZZDQuhSyqmtI6WhfO+I98LVctvBmFY97RI0eZAnkfXtKqXNT0zdW8lqq
g4+RkZ
hpjwemw+RtSVDTTMJERjBIOIwly2Ecy8hfRfipa6D5jsGPkeJzE2JbCZ7Fa
Teg4D
/2sNW73QbG4YbOKmANnFPo7RW5+lIZuI7BN2MSvsqHcaAQ0wR4+UIM
fezlwQ6wsa
+7NShsUlWz2cAI0I3xQyaYc0Y3MR4e1ak6eZDpB0IXPZdgPiLKX59gyF5tx
ZKvth
KqDqCz9DL94jB45p3kRrfkMHiqmYYqqE7VQPpvH+ZZ1u0qwBe3s3GX/77
6xYkRqN
JfhQudQrV5xgQ9BNEQVdOaFkjjg3QG91qYyHRZhap7T4SsOUaARnIHlm
4bsaEoC6
i6npRKs12rgKAiCn9ZwGcegePWAIuNZVDLOBPhFdVJwk7VADjlOPUPJv
ygHQ48oh
MHRvaIUkay1yzYup1/FHok5CBoaLLsSj0xo+wR/QNFUC1rcVQo7x5bXws
A22ykmX
KKGrODiTI8THvdUxTlYZ
=7Nfk
-----END PGP MESSAGE-----

Quote: "I cannot be of much help to you with writing as I am not much help to myself, given my own occupation especially. If you want the Dark Web to help you, you've got to help the Dark Web."
Response: Thanks for the response. I understand give to get.
Here is me giving to the larger community via you.
https://anonfiles.com/D03aMdZdxb/DW_Hosting_pgp
Post where you believe it to be appropriate and helpful.
Can you give me a few minutes now?

-----BEGIN PGP MESSAGE-----
~~ENCRYPTED MESSAGE~~
-----END PGP MESSAGE-----

Note: Фёдор Михайлович Достоевский in his signature in the message above turns out to be a name and translated from Russian is:

> Fyodor Mikhailovich Dostoevsky, sometimes transliterated as Dostoyevsky, was a Russian novelist, short story writer, essayist, and journalist. Dostoevsky's literary works explore the human condition in the troubled political, social, and spiritual atmospheres of 19th-century Russia, and engage with a variety of philosophical and religious themes. Died: February 09, 1881, Saint Petersburg, Saint Petersburg Governorate, Russian Empire – Wikipedia

So n0stis sent off this personal message to IaL, encrypted of course.

I am watching and have been watching how things work across several forums and have found very little to write home about, so to speak.

A lot of vitriol, rampant speculation, condescension and very little help for noobs, advice, or anything approaching a welcoming environment.

If people are on dread to avoid the overbearing moderation of Reddit, its rejection of VPN's and Tor, and questionable security, how long do they last here? Food for thought.

Here is a Pease offering from me.

I have updated the /u/matter original list, removed duplicates, dead links, and introduced some formatting. You may review for errors, and you may use the finished product and post on a sub for info for newbie's if you like.

The document is posted at this site:

https://anonfiles.com/D03aMdZdxb/DW_Hosting_pgp

-----BEGIN PGP MESSAGE-----

~~*ENCRYPTED MESSAGE*~~

-----END PGP MESSAGE-----

What is this file you are sharing me? I do not decrypt files I get from random DN users as a matter of opsec.

Based on the context of your message this a list/guide from u/matter, I'm guessing about hosting .onion sites?

Are you planning to develop something for the DN community or something?

Sincerely,

IaL

Quote: "Based on the context of your message this a list/guide from u/matter, I'm guessing about hosting .onion sites? Are you planning to develop something for the DN community or something?"

matter has already received and thanked me for it.

It is an unencrypted pdf inside a zip, so I encrypted only the link to you.

"Obviously I might have said it in a slightly more uncouth manner of course, but it wouldn't be the darknet otherwise."

So we get back to the DW being a less hostile environment if you want it to grow and prosper.

"You don't seem to be the usual type of user I normally run into in this part of the internet and I only meant to tell you that those kinds of questions might come off as suspicious to some users."

Response: So time for me to come clean as well.

I am a writer doing research for a historical novel about the Dark Web. I am not a journalist, but I am looking to have discussions with a number of people on a number of topics on dread, The Hub, and maybe Envoy.

I think that you as a dread subscriber would be a good choice for me if you are willing. I am not looking to expose anything other than get some ideas of who and why people are here and what they are doing. Am interested in legal activities only. This is nonnegotiable.

I am looking to have discussions on these topics and others.

The Dark Web provides:

Freedom of or from politics?

Less moderated discussions of world, national, or life events

Freedom of or from Internet advertising

Freedom from or of Internet surveillance

Freedom of or from religion

I am also available at:

Email n0stis@mail2tor.com if you would prefer a less clunky format.

At this point, I am 120k words and 600 pages into this manuscript with will eventually be split in two very expansive books unlike anything previously written. The first is a novel, Tales from the DW (what it is, how to navigate it, and what and who is there), and the second book will be full of highly technical DW and OpSec detail and preliminarily called the 42nd and Final Encyclopedia of Cyberspacia for the Imperial Library of Trantor.(grin).

I have no ill will or ill intent towards anyone or anything. n0stis

-----BEGIN PGP MESSAGE-----

~~ENCRYPTED MESSAGE~~

-----END PGP MESSAGE-----

Hi,

In that case let me apologize for my manners. You don't seem to be the usual type of user I normally run into in this part of the internet and I only meant to tell you that those kinds of questions might come off as suspicious to some users.

Obviously I might have said it in a slightly more uncouth manner of course, but it wouldn't be the darknet otherwise.

(/u/IamLegion): ------BEGIN PGP MESSAGE-----

Version: GnuPG v1

~~-----ENCRYPTED MESSAGE~~

-----END PGP MESSAGE-----

Hi,

To answer your question what the darknet means to me is just a place I can go online to be myself.

Evidently in the era of social media having a user's identity connected to an account leads people to be fake about the things they talk/post about... ironically, being anonymous seems to encourage people to be more themselves.

The darknet is chaotic to be sure but it is a beautiful mess, and it gives you a peak of raw uncesored human nature, both the good and the bad aspects.

For instance in Dread, the fact that we are self regulating and have unanimously agreed that child pornography is unacceptable is something of a testament that we do not need laws to tell us what is right or wrong. There is even a community for harm reduction and scam protection, it is a sight to behold.

Unfortunately I regret to inform you that I am neither interesting enough of a user nor am I willing to be in your manuscript.

However, I do find your endavour to be worthwhile and so may I recommend that you approach these two characters:

1.) /u/We_Are_9000

2.) /u/Pygmalion

> *"The two are polar opposites of each other but both are very interesting characters and I would say are integral to the Dread community."*

Feel free to reach out to them on Dread, tell them IamLegion sent you, they already know you're coming and what you are trying to do.

I wish you good fortune in your endeavour, and please, when this work of yours is done do share it with the community or to me at least.

You can reach me here on Dread anytime.

Thanks,

IaL

p.s.

/u/We_Are_9000's public PGP key on Dread is no good, use the following to encrypt your message for him:

~~*BEGIN PGP MESSAGE*~~

~~*ENCRYPTED MESSAGE*~~

~~*END PGP MESSAGE*~~

My response:

IaL,

I appreciate your response and answers and I really appreciate your referrals as it indicates a level of trust.

You did not comment on the DW hosting doc however.

What I have seen too much of on dread and the hub for that matter, is mods and users who act like snipers shooting snark and condescension at every one who looks like a noob, or shows any evidence of an intellect or articulation of the English language by simply daring to ask a question.

You in fact, actually write quite well in this message format.

They frequently display the ignorance of arrogance, and hurt the forums OpSec not improve it. This kind of browbeating does not improve the OpSec of the DW in general.

I anticipate uploading my finished works to the Imperial Library. I have already reached out to them regarding accepting pdf files so I don't have to mangle my writing and formatting by feeding it into a digital sausage grinder to create an ePub. No response yet.

http://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd-4xzt26ochei4m6f7tayd.onion/

Then he got another response from IaL.

Another response from IaL,

Dear n0stis,

Quote: "I appreciate your response and answers and I really appreciate your referrals as it indicates a level of trust."

Response:-You are welcome, I see the value in your work now that you have elucidated me on the matter. I hope the referrals will be an asset to your work.

Quote: "You did not comment on the DW hosting doc however."

Response:-Regarding the DW hosting doc, I tried decrypting the file I got from your link but it failed because it says I do not have the secret key for it.

Quote: "What I have seen too much of on dread and the hub for that matter, is mods and users who act like snipers shooting snark and condescension at every one who looks like a noob, or shows any evidence of an intellect or articulation of the English language by simply daring to ask a question."

Response:-I think it is a given that if you are easily offended and/or triggered by a bunch of words or images then the internet will not be a fun place for you. Even on the clearnet with all its moderation it is still the case, how much more on here? There are users on Dread that I help and berate at the same time, but that is just me welcoming them to the darknet. Do not expect anything out of anyone out here, you will have a better time. Also in their defense (and mine) alot of the answers these people are looking for can be found easily if they just put in some time and effort to find it, which is the kind of mindset expected from darkneteers.

Quote:"They frequently display the ignorance of arrogance, and hurt the forums OpSec not improve it. This kind of browbeating does not improve the OpSec of the DW in general."

Response:-I think it is a social filter, if a user is not competent enough to figure things out on their own then it might be best to leave him/her out in the cold. You might think it is harsh but we can only go as fast as our slowest member, so I tihnk it is better we cut some of the slower ones loose. Also I think there is a kind of recentment from the OG darkneteers when back in the day nothing was given to them, no guide no nothing, they literally had to figure things out from the bottom up. Now a days, not only are there guides for new users but they expect everything to be handed to them or even done for them, which ironically is the reason why a lot of people get phished or scammed because every now and then an opportunist sees an opening and hands them a shiny poisoned apple, and the new users gladly take big bites out of that mother fucker. We can't protect people from their own stupidity, I think you would agree.

I look forward to reading your work once it has been uploaded to the Imperial Library, good luck!

Sincerely,

IaL

IaL,

Response: The download link should have given you an unencrypted zip file and extracting (7zip or something like it) it will reveal an unencrypted pdf file I can email it if you give me an address.

Am waiting to hear from your two referrals.

I am a big boy and have seen plenty online since 2400bps dialup days. It just seems unnecessary, there is more than enough hatred and division offline. It doesn't cost anyone anything to be kind.

Easy is subjective based on experience, and I have done tech support for 30 plus years. I try to not be like Nick the computer guy from SNL.

If we could apply your Darwinian theory to the real world, 1 million US (mostly after the vaccine) and 15 mil worldwide wouldn't have needed to die

from COVID. Mostly males however and that does clean up the gene pool a bit, however bad that sounds.

Writing books takes a long time. The last one was four years.

n0sits (who remembers needing to load separate print and screen drivers each for WP, 123, and dBase back in the day.

IaL,

Ok, so I maybe screwed up on the document link. So I will try again: https://anonfiles.com/n2q6Ddd3y3/DW_Hosting_pdf

After a rocky start, I am starting to communicate with Rorschach_9000. No word from Pygmalion as of yet.

Meanwhile I have formed a few more questions and can't help myself but to share them with you.

My impressions across several months is that the DW I have seen, dread, The Hub, Envoy and a few others are mostly about drugs. Is that a valid impression?

Are there other places you would recommend that I visit to expand my view of the DW?

There is a lot of conjecture in the forums about LE scraping dread. Do you believe this to be real or imagined?

Or is LE scraping the entire DW?

Do you think that Memex (NSA google) is a real thing?

Thanks,

n0stis

So n0stis sent off a couple of encrypted messages:

Hello /u/We_Are_9000 (Rorschach_9000), /u/Pygmalion

As I mentioned to /u/IamLegion, I am n0stis and am a writer doing research for a historical novel about the Dark Web. My two previous as of yet unpublished books are PC/Internet technology related and cover a 40 year historical period-1974 to 2014.

This third book will pick up from there and be exclusively about Cyberspace.

I am not a journalist nor will any of the characters written about be real.

These are the initial questions I have formulated for my research.

Who am I and why am I here?

The Dark Web provides:

Freedom of or from politics?

Less moderated discussions of world, national, or life events?

Freedom of or from Internet advertising?

Freedom from or of Internet surveillance?

Freedom of or from religion?

With my interest in producing both a novel with fictional descriptions of who and why people are there and what they are doing, legally. I will also introduce some first person semi-humorous stories within this book describing the hero's quest for a free and safe place in Cyberspace, out of the reach of corporations, governments, and their surveillance and ad driven autonomous algorithmic AI's.

Also because of my extensive technical research, mostly complete, I hope to also produce a technical guide or encyclopedia for both new and experienced DW user community to be housed in the DW Imperial Library collection on Trantor. Or in this galaxy at:

http://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt-26ochei4m6f7tayd.onion/

Now knowing my goals and intentions, what additional or different questions do you think I should be asking? Are the one's listed the right approach?

IAL mentioned that what the Dark Net means to him is a place he can go online to be himself without his user identity connected to an account. He believes that this identity connection leads to people be phony about the things they talk/post about, and that being anonymous seems to encourage people to be more themselves, self-regulate, and look out for each other. He told me that he finds you to be both interesting and integral to the DW.

This is total anonymity effect is actually the opposite of what most people believe so this is an interesting take to me. This type of total anonymity is however what Web3 is about from what I have read and heard from Gavin Wood and Harry Halpin for some examples. You can tell I am a writer because I tend to ramble on...

I would prefer to communicate via email, unless you believe that messages in dread are better OpSec, I will let you make that judgment. I am n0stis@mail2tor.com.

I am willing to obtain an elude.in or other account if you like.

I have no ill intent towards anyone or anything.

Thank you in advance for your participation, and your patience in reading this,

n0stis

Tried to log into dread, but got this instead:

The 500 error code is a generic message that appears when something unexpected happened on the web server and the server can't offer more specific information. Rather than giving you a normal web page, an error occurred on the web server and the server gave your browser a web page with an error message instead of a normal web page.
However, if the server has installed Microsoft Internet Information Services (Microsoft IIS)[54], the error code will be specified. Decimal places indicate the cause of the error in more detail:
• 500.0: Module or ISAPI error occurred. For example:
• 500.11: Application is shutting down on the web server.

Then he finally did get logged in and received a response to his previous message with an error.

Quote: (/u/We_Are_9000): The key on my profile is not valid, here is my current key....

Response:

Sent this in the clear, on dread of course.

IaL already sent me the new one, but i tried to reimport it anyway and got this:

0 key(s) imported successfully, 1 key(s) import error

Rorschach_9000 <meff_god_9000@elude.in>

This key was already added

Do not know what to say at this point.

Will try to send an email, but do not know if Tor email is operable across different ISP's.

n0stis

Then a response from IaL,

Dear n0stis,

Quote: "After a rocky start, I am starting to communicate with Rorschach_9000. No word from Pygmalion as of yet."

Response:- will probably get back to you within the week, he/she/they go awol randomly for short periods, its the darknet people disappear all the time.

Quote: "My impressions across several months is that the DW I have seen, dread, The Hub, Envoy and a few others are mostly about drugs. Is that a valid impression?"

Response: -drugs bring the most economic activity to the darknet and so a proportionate amount of resource is allocated to the subject matter

Quote: "Are there other places you would recommend that I visit to expand my view of the DW?"

---

[54] Note: This is unlikely on the Unix (Linux) based DW.

Response: -nowhere that would be of interest to you that involves legal activities

Quote: "There is a lot of conjecture in the forums about LE scraping dread. Do you believe this to be real or imagined?

Or is LE scraping the entire DW?"

Response: -In my opinion there is a high probably of this being the case, it requries very little resource for them to do this. From my perspective it is better/safer to assume that this is true because if we are wrong at least we are erring on the side of caution.

Quote: "Do you think that Memex (NSA google) is a real thing?"

Response: -I do not know what you are referring to. Is this a reference to a conspiracy theory?

Thanks,

IaL

IaL,

Thanks for the response.

I am having trouble with the keys from both 9k and Pygmalion (Pygmalion Envoy Moderator Jr. Member) and only have messages that I cannot encrypt from both. I have responded to this problem via email, so we shall see. I hate to use dread messaging unencrypted as it may get deleted by a mod.

Quote: "Do you think that Memex (NSA google) is a real thing?" -I do not know what you are referring to. Is this a reference to a conspiracy theory?"

Response: Supposedly the NSA has a google for the DW called Memex. Am having difficulty finding info about it, so I thought I would ask you.

On another note: I have been banned from The Hub. They were giving me a hard time over there sniping at me, so I thought I would try to join in as you can see below:

I was asked an incoherent question regarding my quoting practices on messages and I responded by saying it was a dumb question asked by a drug addled moron with a room temperature IQ, and then asked if I fit in with the group now. It was the last thing I did there.

Any advice?

How to join with another username?

How does the site know who I am before even logging in?

Thanks,

n0stis

Message content to and from /u/We_Are_9000

Hello /u/We_Are_9000 (Rorschach_9000)[55]

As I mentioned to /u/IamLegion, I am n0stis and am a writer doing research for a historical novel about the Dark Web. My two previous as of yet unpublished books are PC/Internet technology related and cover a 40 year historical period-1974 to 2014.

This third book will pick up from there and be exclusively about Cyberspace.

I am not a journalist nor will any of the characters written about be real.

These are the initial questions I have formulated for my research.

Who am I and why am I here?

The Dark Web provides:

Freedom of or from politics?

Less moderated discussions of world, national, or life events?

Freedom of or from Internet advertising?

Freedom from or of Internet surveillance?

Freedom of or from religion?

With my interest in producing a novel with fictional descriptions of who and why people are there and what they are doing, legally. I will also introduce some first person semi-humorous stories within this book describing the hero's quest for a free and safe place in Cyberspace, out of the reach of corporations, governments, and their surveillance and ad driven autonomous algorithmic AI's.

Also because of my extensive technical research, mostly complete, I hope to also produce a technical guide or encyclopedia for both new and experienced DW user community to be housed in the DW Imperial Library collection on Trantor. Or in this galaxy at:

http://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt-26ochei4m6f7tayd.onion/

Now knowing my goals and intentions, what additional or different questions do you think I should be asking? Are the one's listed the right approach?

IAL mentioned that "what the Dark Net means to him is a place he can go online to be himself without his user identity connected to an account. He believes that this identity connection leads to people be phony about the things they talk/post about, and that being anonymous seems to encourage people to be more themselves, self regulate, and look out for each other. He told me that he finds you to be both interesting and integral to the DW."

This is total anonymity effect is actually the opposite of what most people believe so this is an interesting take to me. This type of total anonymity is

---

[55] Hermann Rorschach, a Swiss psychiatrist, Rorschach test, his psychological evaluation method involving inkblots, Rorschach (character), a character from the comics Watchmen. It could be any of these but I suspect the later.

however what Web3 is about from what I have read and heard from Gavin Wood and Harry Halpin for some examples. You can tell I am a writer because I tend to ramble on...

I would prefer to communicate via email, unless you believe that messages in dread are better OpSec, I will let you make that judgment. I am n0stis@mail2tor.com.

I am willing to obtain an elude.in or other account if you like.

I have no ill intent towards anyone or anything.

Thank you in advance for your participation, and your patience in reading this,

n0stis

He received a dread encrypted PM which could not be read, so he sent an encrypted Envoy PM.

9k,

Saw you here so I thought I would message since I cannot read your PM key on dread.

Not trying to bug you, just let you know I can't read your answers to my initial questions.

Thanks,

n0stis

/u/We_Are_9000

I have not sent you any encrypted messages!!!!!

if you want my knowledge get jabber!!!!!

You are wasting my time!!!!!

Quote: "I have not sent you any encrypted messages!!!!!"

Response: I guess it was just your PGP key.

Quote: "if you want my knowledge get jabber!!!!!"

Response: Not looking for your _knowledge_. Just looking for some of your impressions about the DW.

Quote: "You are wasting my time!!!!!"

Response: And you mine as well, so I will give your demand a HARD PASS for reasons I already explained. And also real time communication does not fit my own personal OpSec requirements, nor is it a good use of my time.

n0stis

It is very interesting to me that with all the talk from these guys about OpSec, that they use private email and not Tor email. They also want to chat over encrypted, but real time jabber chat apps.

Quote: "Are you sure you understand how to use pgp? Because this last message is no good. Why the fuck are you even using it??? Either get an encrypted im or use Tutanota email

Meff_god_9000@tuta.io No need for pgp"

Response: I am not sure that you mean to come off as harsh as you are.

I have been exchanging messages successfully with IaL and Pygmalion using PGP on dread for some weeks now.

Search came up tutanota.com. Can you give me an onion link?

I have only been using, and wish to use only Tor email.

I will also try to send this same message via another domain, in case this one does not work. Relay not permitted.

As I previously mentioned, among other things, I am looking to discover who is on the DW, why, and what they are legally doing and why. IaL said that you could offer a unique perspective.

I intend no harm to anyone or anything.

Thanks,

n0stis

"Are you sure you understand how to use pgp? Because this last message is no good.

Why the fuck are you even using it???

Either get an encrypted im or use Tutanota email

Meff_god_9000@tuta.io

No need for pgp"

I discovered a few things since I replied to you via email:

Currently, Torbox only supports emails to and from lelantos.org, maskedmail.com, mail2tor.com, mailtor.net and safe-mail.net.

So I could not get a message to you via TorBox. I did send the same one with my elude account, which uses CAPTCHA and also PGP for 2FA.

I looked at https://mail.tutanota.com/ and it requires JavaScript, so that is a nonstarter for me.

n0stis

Email is not always working across domains.

From: "Mail Delivery System" <MAILER-DAEMON@torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion>

To: n0stis@mail2tor.com
Subject: Undelivered Mail Returned to Sender
Date: 2022-05-13 04:24 PM
Attachment:
Part 3 2 kB
Character encoding:
This is the mail system at host torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion.
I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.
For further assistance, please send mail to postmaster.
If you do so, please include this problem report. You can
delete your own text from the attached returned message.
The mail system <pygmalion@secmail.pro>: connect to secmail63sex4dfw6h2nsrbmfz2z6alwxe4e3adtkpd4pcvkhht4jdad.onion[0.0.0.1]:25: No route to host

Note: Currently, TorBox supports emails to and from lelantos.org, maskedmail.com, mail2tor.com, mailtor.net, and safe-mail.net.

Hey,
Response: Please keep a full log of the conversation like I am doing. That way it's easy to read back on what was said before and you only have to decrypt one single message to read all that was said. :)
I am very busy, so I don't have time to go back and read previous messages.
Sorry to hear you are in need of self-therapy. I applaud you finding the strength to go through with it.
For me, it's the same. A shaman is in some American tribes is traditionally the one requiring most healing, and he achieves it by healing others.
/d/Council is inactive mostly because I don't have the time and strength to carry it any more and there is a lack of other leading personalities willing to pick it up.
Essentially, /d/council represents Freemason principles. If you want to understand the motivation behind it, study the Freemasons.
Piratepilot is way out there, yeah. They're the manifesto-writing kinda person.
Sincerely,
Pygmalion
Response: Ok, I will keep the full convo. I was just quoting the relevant parts like I usually do on the Clear Web. Just a habit.

I meant therapy in the loosest sense, like in order to get something off my mind I have to write about it or it nags at me. Seems to be more of that every day now.

This is an example:

This is an excerpt from the Prologue for my new book.

The wealthy who reveled in their decadence earned from their predatory thievery now having obtained a majority of the total money, engaged in the unaccountable plundering of the planet's resources and the eminent domain capture of the property of the world. Their corporations continued their Manifest Destiny of war driven empire building, war profiteering, dystopian global surveillance, and their parasitic digital data collection machines to exploit, commercialize, and commoditize human online life for limitless wealth. They passed this wealth from generation to generation, each generation believing that they were inherently smarter and more deserving. It was as if being born on third base carried with it the assurance, that they had hit a standup triple. This was the primary source of their unwarranted and naïve optimism. With power and wealth, they have created their own personal narcissistic blue pill reality.

I learned a life lesson from the Native Americans. Their rain dances never failed to work. It was not due to magic or the great spirits, but it was their persistence. They did not stop dancing until it rained. <g>

I am not one for organized institutions, especially religion, am far too independent which caused me some amount of trouble in school and the military.

PS. am still curious about DW databases if you know anything.

PPS. I sent you an email from TorBox to secmail.pro. It bounced. What do you know about interoperability of Tor email domains?

Thanks,

Then IaL messaged.

Dear n0stis,

Quote: "I am having trouble with the keys from both 9k and Pygmalion and only have messages that I cannot encrypt from both. I have responded to this problem via email, so we shall see. I hate to use dread messaging unencrypted as it may get deleted by a mod."

Response:-That is strange, did you previous messages decrypt properly and only now did it become an issue? And yes it is always a good idea to encrypt personal correspondence, mods in the darknet are generally suspicious of people who ask too many questions

Quote: "Supposedly the NSA has a google for the DW called Memex. Am having difficulty finding info about it, so I thought I would ask you."

Response:-I do not have any input on this matter, maybe I will look into this

more sounds like an interesting topic

Quote: "I was asked an incoherent question regarding my quoting practices on messages and I responded by saying it was a dumb question asked by a drug addled moron with a room temperature IQ, and then asked if I fit in with the group now. It was the last thing I did there."

Response:-Hahahaha! Good one, someone got butt hurt!

Quote: "How does the site know who I am before even logging in?"

-it shouldn't, tor doesnt keep sessions alive and you are given a new identity everytime you launch it, that is strange. Also, I am not active on the Hub

Sincerely,

IaL

IaL,

Response: 9k eventually sent me a dread clear message telling me that he would only talk to me on Jabber and I responded encrypted and declined.

I am still digging on Memex as well. Meanwhile there is a new encryption standard that NSA had a hand in. What could possibly go wrong with that?

I got back into the hub with a new username, but there is so little there of interest it is mostly a waste of my time. Same with Envoy.

I am still curious about DW forum and market databases if you know anything. Open source MySQL, SQL Express or something. Need info for the book. Also, what do you know about interoperability of Tor email domains? I am confused on who can send to who.

Appreciate your help.

Dear n0stis,

It is unfortunate that you decided not to come through with 9k, he would have been a nice contrast to Pygmalion. Were you able to get intouch with Pygmalion though?

Memex would be an interesting topic right now especially with the new drama unfolding in Dread about some markets being hacked and/or operated by LE. I think it is safer to just assume that LE has infiltrated Dread and most DNMs and mitigate risk by proper opsec. I wonder what is it that LE is after though, stopping the trade of illegal goods is a given but maybe there is something else in the darknet that interest them?

Regarding DNM databses I am not sure what stack they are using as I am a clearnet developer, SQL is not one of the competencies of my tech stack, I work with document model databases.

On TOR email domains you should have no problem with interoperatbility, however it is my understanding that some services are TOR only.

Sincerely,

IaL

Quote: "It is unfortunate that you decided not to come through with 9k, he would have been a nice contrast to Pygmalion. "

Response: I didn't like his demanding attitude and use of several exclamation points.

I don't think he will change his mind about chat and that is a deal breaker for me.

Pygmalion is part of a syndicate. So is 9k opposite of that? Can you give me a hint?

Quote: "Were you able to get intouch with Pygmalion though?"

Response: Yes we have exchanged a number of messages and I now know far more about that lifestyle and those attitudes than I ever wanted to. Yikes!

IaL: "I wonder what is it that LE is after though, stopping the trade of illegal goods is a given but maybe there is something else in the darknet that interest them?"

Response: Inquiring minds...

IaL: "Regarding DNM databses I am not sure what stack they are using as I am a clearnet developer, SQL is not one of the competencies of my tech stack, I work with document model databases."

n0stis: Ok, thanks I also asked Pyg.

IaL: "On TOR email domains you should have no problem with interoperatbility, however it is my understanding that some services are TOR only."

n0stis: So far I have only been able to email from torbox to elude. Still trying to figure it out.

Sincerely, n0stis

Contact with /u/Pygmalion

Note: Pygmalion is best known as the Greek mythological figure. In ancient Greek mythology, he is a legendary figure of Cyprus, who was a king and a sculptor, and who fell in love with a statue he had carved, which then came to life. Wikipedia

Dear n0stis,

Thank you for reaching out. I am the admin of the Pygmalion Syndicate. We sell drugs.

IAmLegion mentioned that you want to discuss legal things only, so I put that out there right away for your consideration. I've also been involved in some non-profit things such as /d/Council.

I'll sent you an email from pygmalion@infantile.us and respond here as well in case the email does not get through.

Who am I and why am I here?

To give the following quote power:

> *"I, as a responsible adult human being, will never concede the power to anyone to regulate my choice of what I put into my body, or where I go with my mind. From the skin inwards is my jurisdiction, is it not? I choose what may or may not cross that border. Here I am the Customs Agent. I am the Coast guard. I am the sole legal and spiritual government of this territory, and only the laws I choose to enact within myself are applicable" Alexander Shulgin*[56]

Quote: The Dark Web provides:

Response: Galt Gulch

Note: An online community for Ayn Rand and Atlas Shrugged fans, yikes!

Quote: Freedom of or from politics?

Response: We have our own politics.

Quote: Less moderated discussions of world, national, or life events?

Response: We have our own moderation.

Quote: Freedom of or from Internet advertising?

Response: We have our own advertisements.

Quote: Freedom from or of Internet surveillance?

Response: Surveillance is everywhere, even here. Be careful about what you reveal about yourself.

Quote: Freedom of or from religion?

Response: /d/SpiritualHealing

Sincerely,

Pygmalion

Quote: Dear n0stis,

Thank you for reaching out.

I am the admin of the Pygmalion Syndicate. We sell drugs. IAmLegion mentioned that you want to discuss legal things only, so I put that out there right away for your consideration."

---

[56] Alexander Theodore "Sasha" Shulgin (1925 – 2014) was an American medicinal chemist, biochemist, organic chemist, pharmacologist, psychopharmacologist, and author. He is credited with introducing methylenedioxymethamphetamine (MDMA, commonly known as "ecstasy") to psychologists for psychopharmaceutical use and for the discovery, synthesis and personal bioassay of over 230 psychoactive compounds for their psychedelic and entactogenic potential. Due to Shulgin's extensive work in the field of psychedelic research and the rational drug design of psychedelic drugs, he has since been dubbed the "godfather of psychedelics".

Response: I appreciate your trust and response. As you can see I am reading this fine now. It is easy to make mistakes with this encrypted format, I have made many myself, so I will email you as well with some additional questions.

I am aware of your presence on Envoy, not aware of a Syndicate nor do I care at this point. I will check out /d/Council, thanks for the tip.

Introductions by /u/Pygmalion • in /d/Council

To break the formality of this board a little bit, every member is invited to introduce themselves here in this post and tell us a little bit about themselves and why they are here. No ads though, please. You may link to your platform or subdread, that's it. I'll make a start: I am the head administrator of the Pygmalion Syndicate (/d/Pygmalion).

The Pygmalion Syndicate is a team of renegade hippies who has been around vending stuff for a while. We also made some substantial contributions to Dread, including /d/SpiritualHealing and /d/vendor_handbook. Our primary goal is to spread love and kindness wherever we go. :3

Thank you

edit: This is for official members, but I guess everyone who wants to can post as well because why not.

The Council is a non-profit organization for freethinking and good people on the darknet. Any reputable person is welcome to apply and contribute.

The purpose of the Council is to educate, to be honorable, and to create alliances in order to build an open source society.

Members are expected to reperesent these goals wherever they go.

/d/Council

289 subscribers

http://dreadytofatroptsdj6io7l3xptbet6onoyno-2yv7jicoxknyazubrad.onion/d/Council

My intro message on /d/council,

Hello, I am n0stis. I am a writer doing research for a historical novel about the Dark Web. I am not a journalist, but I am looking to have discussions with a number of people on a number of topics.

With my interest in producing a novel with fictional descriptions of who and why people are there and what they are doing, legally. I will also introduce some first person semi-humorous stories within this book describing the hero's quest for a free and safe place in Cyberspace, out of the reach of corporations, governments, and their surveillance and ad driven autonomous algorithmic AI's.

Also because of my extensive technical research, I hope to also produce a technical guide or encyclopedia for both new and experienced DW user community to be housed in the DW Imperial Library collection on Trantor. Or in this galaxy at: http://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt26ochei4m6f7tayd.onion/

I have no ill intent towards anyone or anything.

Hello Pygmalion

I appreciate your answers and will take some time to digest them.

I am less concerned about revealing myself as much as necessary to have these kind of honest conversations, since I will not be buying crypto or doing transactions.

Thank you again, n0stis

Via emai: pygmalion@infantile.us via torbox

Am sending this unencrypted, but I you want to use it respond that way.

My impressions across several months is that the DW I have seen, dread, The Hub, Envoy and a few others are mostly about drugs. Is that a valid impression?

Are there other places you would recommend that I visit to expand my view of the DW other than /d/council?

There is a lot of conjecture in the forums about LE scraping dread. Do you believe this to be real or imagined?

Is LE scraping the entire DW?

Do you think that Memex (a rumored NSA Dark Web google) is a real thing?

Thanks again,

n0stis

An error occurred : : DATA:250 2.1.0 Ok | DATA:550 5.1.1 <pygmalion@infantile.us>: Recipient address rejected: Relay not permitted. Check out current peering at http://torbox3uiot6wchz.onion/relay-en.php | DATA:250 2.1.5 Ok | DATA:250 2.1.5 Ok | DATA:250 2.1.5 Ok | DATA:354 End data with <CR><LF>.<CR><LF> |

Then n0stis sent via elude and it seemed to go. No errors, copied to my TorBox address just fine, but not viewable in elude as Sent. This reminds him how much he really hates this web mail shit, and needs to get a Tor email address for him.

Subject: Re:
From: "Kaizu Shibata" <kaizushi@infantile.us>
Date: Fri, May 27, 2022 21:38
To: arister0s@elude.in

I would like a background on you and your work to research. Links to blogs, comments, and discussions will help me establish if you are actually the real deal.
On Fri, 27 May 2022 17:11:52 +0000
arister0s@elude.in wrote:
> "Secure Email
> Infantile offers an exclusive mail service only for the dark web's
> best and brightest. Use the contact details for kaizushi below if you
> think that is you."
>> Hello,
> I am looking for a secure email to use for correspondence. I am very
> frustrated with TorBox, elude and Proton mail.
> I am n0stis and am a writer doing research for a historical novel
> about the Dark Web. My two previous as of yet unpublished books are
> PC/Internet technology related and cover a 40 year historical
> period-1974 to 2014. This third book will pickup from there and be
> exclusively about Cyberspace. I am not a journalist nor will any of
> the characters written about be real.
> With my interest in producing a novel with fictional descriptions of
> who and why people are there and what they are doing, legally. I will
> also introduce some first person semi-humorous stories within this
> book describing the hero's quest for a free and safe place in
> Cyberspace, out of the reach of corporations, governments, and their
> surveillance and ad driven autonomous algorithmic AI's.
> Also because of my extensive technical research, I hope to also
> produce a technical guide or encyclopedia for both new and
> experienced DW user community to be housed in the DW Imperial Library
> collection on Trantor. I have no ill intent towards anyone or
> anything. Sincerely,
> n0stis

Kaizu Shibata <kaizushi@infantile.us>
Kaizushi's Little Onion Server
https://kloshost.online/
kaizushih5iec2mxohpvbt5uaapqdnbluaasa2cmsrrjtwrbx46cnaid.onion
Subject: Re: email service
From: arister0s@elude.in
Date: Sun, June 12, 2022 16:17
To: "Kaizu Shibata" <kaizushi@infantile.us>
Cc: n0stis@mail2tor.com
Hello,
Sorry for the delay but I have not been able to get logged into Elude is quite some time and they are down more than up.
I would prefer that you respond to my n0stis@mail2tor.com address.
On the DW, I am active on dread as n0stis, especially on /d/OpSec.
On the CW you can see my essays, and short stories at tcw.org.
I am currently writing, offline, a novel and a DW user guide and have attached an outline to this message.
Thank you for your consideration.
arister0s n0stis

Encrypted PM on dread to Pygmalion.
Is there more to the story here?

"Pygmalion is best known as the Greek mythological figure. In ancient Greek mythology, he is a legendary figure of Cyprus, who was a king and a sculptor, and who fell in love with a statue he had carved, which then came to life. Wikipedia"

"The quote you provided, does this sound about right?

Alexander Theodore "Sasha" Shulgin (June 17, 1925 – June 2, 2014) was an American medicinal chemist, biochemist, organic chemist, pharmacologist, psychopharmacologist, and author. Due in part to Shulgin's extensive work in the field of psychedelic research and the rational drug design of psychedelic drugs, he has since been dubbed the "godfather of psychedelics". Wikipedia"
n0stis
Yeah,
Pygmalion is all about love, the right to own one's own body, and education.
https://en.wikipedia.org/wiki/Pygmalion_effect, which pretty much translates to "believe in yourself and you shall succeed".
The prohibition of drugs is a form of oppression. We are not allowed to feel what we want to feel, think what we want to think, experience ourselves and enjoy love without boundaries simply because it threatens the established

authorities. The prohibition of drugs, psychedelics in particular, is a form of thought control. They, whoever "they" may be, want a monopoly on that, if anyone is gonna do it (CIA MK ULTRA). People are waking up. Psychedelics will be legal within our life time, and then we have no more reason to be anyone's enemy but can come out and just be ourselves without the need to hide. :) We want to bring life to the statue.

In that, we agree with much of the political and philosophical thoughts written in the book "Food of Gods" by Terrence McKenna.

We strive to educate others to follow our footsteps: /d/vendor_handbook. It may come the day on which Dread will announce that armed warriors broke down our doors, abducted us, stole and destroyed our property, but what will remain are the information we leave behind.

The Alexander Shulgin thing from Wikipedia is correct, though I would like to add that he is a such a powerful influence in our school of thought, that you may call him a prophet of rave culture. He is for rave culture what Hawking is for physics. There are a bunch of these great thinkers. The most powerful, though least mentioned one is Karl Gustav Jung, who predicted much of what was discovered with LSD and was directly opposed to the famous cocaine addict and founder of modern psychology, Siegmund Freud.

I'll leave you with these:

Kaizushi's Revolutionary Hosting Interview @Pygmalion

http://dnhuboxyxgbhmnozl5j4wntoon56x42-3iteusfmbqwsdwl26gnqqy6id.onion/articles/c70ce9a18497

This is an interview by Pygmalion with a guy identified as Kaizushi who runs a DW hosting service among other things. (kaizushi@infantile.us and onion is kaizushih5iec2mxohpvbt5uaapqdnbluaasa2cmsrrjtwrbx46cnaid.onion)

Pygmalion: What do you do out here on the Darknet?

Kaizushi: I call myself a devop. That is someone who works with developers to deploy their products. A developer writes code or automates processes. Perhaps you have heard of sysops, which are system administrators. The result is flexible services to run web application software from a variety of broad open source ecosystems.

Effectively, I am the one you call when you have or need software that you would like to run remotely, anonymously, and securely.

Pygmalion: What are your qualifications?

Kaizushi: The best thing about buying hosting and not doing it yourself, and the same is with my services. You can focus on your software, while I make sure the hardware runs smoothly and securely. Basically, within what I've allowed configuring the systems gives you the freedom as a developer to innovate without risk.

On top of that, it is cheap and efficient to pool resources. A hosting customer has a HTTP proxy to Infantile as basically a private exit to share for using APIs (such as ones protected by Cloudflare) that don't work on Tor exits. The server itself is highly optimized and your hosting account has a lot more resources available than a VPS of similar price.

It's not just my skill you're buying, we have a team. I have pentesters, hackers, and others experienced with Hidden Services consulting with me, such as Cyrus. I have always been open to chat with critics about improving things.

Pygmalion: How do you run it?

Kaizushi: The hardware is best kept mostly as a mystery; however, I have a dedicated server in a secure location and it's reasonably powerful. I have some other servers which are used to get daily backups. If something does happen to the primary dedicated server, I can get a new one online rapidly using the backups.

Pygmalion: What kind of customers do you accept and expect?

Kaizushi: Pretty much anyone, except for people in child pornography. I have a 'violent politics' rule of sort, which is mostly about terrorism. I have never had either sort use my servers. I mostly get business-oriented customers, both legit, and some in fraud. I do not do much about scams, because I don't want to micromanage those sort of things. It is for the market and other services to decide what is good and bad, legit and scam, I try not to get involved. I am happy as long as people are not being exploited or physically harmed.

Pygmalion: Are you not scared to break the law?

Kaizushi: Not at all. I have things set up where I don't even give the law much thought. All the laws outside this place, 'in real life' as people say, are corrupted and I offer a haven from that. The very purpose of what I do is to help people ignore the law as I do. And help protect freedom of speech.

Pygmalion: Laws are corrupted by whom?

Kaizushi: That is a really difficult question if I am not to give an obvious answer. I could say politicans but so might anyone. Though, to get philosophical the issue is that the law is upheld without consistency, from a mixed democratic mandate. The police enforcing it clearly get thrills from violence that corrupt them. The politicans sell society down the road for personal benefit.

Yet I don't really think selfishness is the problem either. The problem is that so many out there in the world bend and flex, and I guess the simplest term for the problem would be hypocrisy. In this world people can bend and flex, but they can't fool a blockchain and we can choose ourselves not to bend. Each of us that acts honestly here is rewarded, and Tor and such keep us safe despite the corruption out there in the world.

Pygmalion: Yeah, I'd say the main issue is that system relevant decisions are generally made based on uneducated opinions rather than axiomatic calculations. Would you say you are part of a revolution?

Kaizushi: Yes, I think if I can provide a stable service, others get the chance to stand for longer. And it is a long battle ahead for freedom. Most revolutions have been violent, and what we are doing on the dark web is actually far more peaceful. We win with honesty and consistency, and not brutality. It is clear to a lot of us that it will reduce violence. The more traditional kinds of revolution, some of those never end and we end up with massively organized tyranny and violence, like China and the Soviet Union. In the case of what we are doing it is more about breaking the cycle than revolving it with blood (revolution) into a new form.

Pygmalion: I'd actually argue that a true revolution can only be accomplished peacefully. If we follow the reasoning of Karl Popper, who said that revolution is the dismantling of incorrect beliefs and creating better ones. We are building a new way of trade and exchange outside of the system. It is a prototype right now because there are many issues that need to be fixed. Scams and downtimes are big ones. Once these issues have been fixed, I am sure we will have more and more people coming in, even from more legal professions.

Kaizushi: I agree. What empowers the individual who is peaceful, regardless of their belief, is what is justice in this world. To put it in other words for the reader, destruction of existing systems creates chaos. Chaos is not revolutionary. Chaos is bad. To be revolutionary there must be a better alternative in place that people will naturally be drawn to; thus, allowing a peaceful transition from a broken system to a new system. Much like many people transition from the Microsoft operating systems to the superior Linux open source operating systems. "Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men." - Ayn Rand (For the new intellectual)

The success of Linux is actually largely from the creative and unique method by which Linus Torvalds decided to control his intellectual property. He revolutionized technology and here we are, taking it from there.

Pygmalion: Where do you think the Darknet is headed?

Kaizushi: Yeah, the predictions, as simple as they are, the justifications and reasons are complicated. A lot would need to be explained, but the predictions are about the future of the drug war and the dark web. There is a lot owed to our current cryptography by civilization, like actually being able to know that torproject.org is controlled. There is the possibility that some governments in fighting the dark web might make a serious attack on any kind of cryptographic trust being possible. In some parts of the world, in future there might only be cryptographic trust for those of us that exchanged public keys well in advance. I doubt it would happen to the whole world, but it certainly

will happen to people in some of it.

Pygmalion: I think cryptography and open source will liberate the entire human race…

Kaizushi: In every war, some battles are lost.

Pygmalion: To drive my point home: Today a destitute guy in Africa still got a smartphone and a working internet connection. He needs cryptocurrencies because his country's currency is based on complete corruption. The true revolution of cryptocurrencies is the replacement of failing currencies that are even more unstable than Bitcoin and Monero.

Kaizushi: The lack of a free society can mean one does not have the freedom to get an OS with integrity. Cryptographic trust implies someone gets an OS with proper SSL CA certs. Without that, they can't actually use the real torproject.org, and get the real Tor browser. It is much the same problem as onion services face with cloners. People with corrupted software, hardware or operating systems can't actually know they are using the real torproject.org

To verify an SSL cert there are CA keys in our browser. If someone doesn't have the real ones, then they can't verify SSL. A lot is owed to torproject.org being recognized as property a nd with LetsEncrypt having contractual obligations. For a long time, SSL certs were expensive and many referred to those who controlled it as the cert mafia. It is much the same problem as onion services face with cloners.

Additionally, we still rely on trust, even out here. My canary on my site, it would be worthless without my right not to incriminate myself, which in America is the fifth amendment. I can refuse to post that canary because of certain legal privileges.

Pygmalion: What happens when you're busted?

Kaizushi: About that, I am not quite sure. I will cross that bridge when it comes to it. What actually lays in my future in this jurisdiction is a takedown notice that has me flee the country like John McAffe, Andrew Aurenhiemer, or Vince Cantfield.

Pygmalion: Any last words for the reader?

Kaizushi: The world we desire, a world of prosperity and peace, is completely possible. It is an issue of philosophy becoming action. One can study and idea and promote it - but it is more important to integrate that idea with our lives and our actions. With cryptocurrency we are living in a time of oppertunity where we can benefit from living by the ideals we think are right. For a long time all we could do is say what is right. Finally, we have the chance to do what is right and be rewarded for it.

Sincerely,

Pygmalion

A Peak Behind the Curtains with William Gibson @Pygmalion - May 20 2021

http://dnhuboxyxgbhmnozl5j4wntoon56x42-3iteusfmbqwsdwl26gnqqy6id.onion/articles/9360e7f60d61

Dear Darknet Community,

I am a small psychedelics vendor and had the opportunity to talk to William Gibson about the newest developments in the Darknet scene. He shared some deep insights to be published here.

Q: What's new with Versus?

What do you think about our new signature drug?

http://j6s7ohobyvhy3jnhocw5agl7iwcmgi5zm3d6isjl62wflufibox4exid.onion/filehost/UtilizeHemlineCytologyHuckleberryAlcohol.zip
http://j6s7ohobyvhy3jnhocw5agl7iwcmgi5zm3d6isjl62wflufibox4exid.onion/filehost/CinchonaSpongiestMarinaWeaponryJute.zip

Yes, it is cocaine, and probably among the best you can get. Another 100 kilos out of the latest shipment. I can't get into details but we already have a few high volume user on Versus which brings me to your next question:

Q: Do you have any plans to help bulk vendors with certain features that don't exist on other markets?

A totally transparent and verifiable multisig[57] payment system is the most important feature we offer to make Versus a viable option for real bulk deals. We are currently the only market with a true multisig solution which is why professionals trust us with literally millions of dollars in escrow. Or more precisely: They don't have to trust us because they can control and verify. No trust necessary. If you lose money it is because you messed up and not because we or anybody else stole it.

Our flexible commission system makes it very reasonable to move bulk business to Versus as we charge proportionally less on bulk deals than other markets with a semi-fixed commission. On high value orders we charge a fee as low as 1% but 1% of a million is still better than 5%-10% of a thousand low value orders.

Locktime transactions are another feature that no other market provides right now as far as I know. Even if Versus goes down vendors will still be able to get their money for all shipped orders after the 90 days locktime. They also prevent situations in which we manipulate payout transactions. We could manipulate them of course but your locktime transactions would still be valid and usable. As long as you verify transactions and signatures, you won't lose any money on exit scams anymore.

---

[57] Multisig A standard bitcoin transaction sends bitcoin to an address. This bitcoin can then be spent by the private key to which it belongs. However, bitcoin can also be sent such that it requires multiple signatures from different private keys.

Q: Where do you think the big changes on the Darknet are right now?

I think the biggest change recently is that finally markets that doesn't keep up the status quo and try to make it all "easy to use" are in charge now. Maybe people are just fed up with half baked markets that only want to steal your coins after a few month of runtime.

Look at White House Market, Monopoly and Versus. We all do things differently. We all do things differently compared to other markets and maybe most important: we go new routes.

A few years ago WHM's monero only and forced PGP policy was unthinkable of. People would just use another market. It is not like nobody ever tried. Look at Libertas Market for example. However Monopoly with its userless direct deal system and in depth vendor vetting is something new that has never been done before as far as I am aware. Versus forced multisig isn't new either but its exactly what the darknet needs with the current exit scam industry. I believe if we could fuse those 3 markets together we would have THE DNM standard of the future.

There will be a market in the future which will build on top of the base we provide right now. New standards. Higher standards. Once forced PGP and XMR Multisig among other features become the norm there will be less "easy to use" shitmarkets around praying on your coin. Less exit scams means a healthier ecosystem. Protecting vendors is good for everyone because on the long run its the user who suffers from exit scams even more than the vendor.

Customer who think vendor protection doesn't benefit them and that multisig only really benefits vendors totally miss the point. Due to their laziness to use mulsisig, vendors lose a lot of money each year but ultimately it is the customer who pays the bill. One way or another a vendor has to make up for all the lost money and customer pay the price either literally by paying more for product or by getting inferior quality product. Multisig is healthy for the whole ecosystem and the only way to end this shitshow of an exit scam industry.

I don't want to badmouth any specific market but the "easy to use" thing is exactly not what this whole business should be about and the only reason markets still go this way is because of laziness and greed aka fast-money, preferably within a year or two and then run away with the escrow pot. Their priority is not to provide a secure platform but to get as many users and vendors in a short time and build up the escrow amount. Look at the last 2-4 years and think about how many markets exit scammed in that short time frame then think about how many of them labeled themselves as "easy to use". Even relatively promising markets.

This is not amazon and we are not selling cookies (most of the time). There should be a certain entrance barrier. Not every child and/or complete retard (please excuse the non-PC-baby lingo) should be able to buy heroin on the internet. Using PGP or BTC MS is not exactly rocket science and you sure

don't need a Ph.D in computer science to learn it either. You don't even need a high school degree. I would claim that EVERYBODY with a somewhat working brain is able to learn both PGP as well as multisig in less than a day IF they really wanted to. If you really can't wrap your head around it, you are mentally probably not mature or healthy enough to use certain drugs in the first place. I am not putting myself in a position to judge about who should or shouldn't consume drugs though. All I say is people who buy drugs should have a certain understanding on how it works around here. It's not a funny video game where you can restart if something goes wrong. People should start to take this whole thing serious for everyone's sake. Lives depend on it. Lazy customer endanger not only themselves but also vendors and markets. If all this Tor, PGP, Cryptocurrency talk confuses you why don't they just go to their local corner boys to buy what they want? They are "really easy to use", total no-brainer. Cash for drugs - deal done. I mean where to draw the line? Isn't it already too complicated to use crypto at all? It is easier to just wire money from your bank account or paypal right? And tor? Why download an extra browser. How complicated. All this hidden service stuff. Why not clearnet markets where we can shop from within an app on our fancy iPhone? You get my point I guess.

Q: I feel like mr_white's move to close vendor registrations was a brilliant idea because the vendors on his market are likely able to serve more customers coming in. That means the pie is getting bigger as well as the pieces on his market. That builds a rich and quality vendors brand for WHM.

That was indeed a good move. We planned to go private as well as soon as we hit a certain benchmark. It is just the way to go and makes not only the support work easier for the staff but improves the quality of the whole market in general. However we wouldn't close down completely. New vendors would still have a chance to apply if high level customer vouch for them. Pretty much how CGMC worked.

Q: What is the DDOS situation right now?

Believe me the DDOS shitshow is still a thing partly thanks to ***a certain ex-exit scam market*** *and their tireless efforts to cripple other markets for their benefit. You just don't notice it that much because we all learned a lot and to be honest we have to credit the Tor project the most because they actually really fixed a lot of issues and made it a lot harder to ddos now. Not impossible but a lot harder.*

Q: Thanks for all the content. It's really good stuff. Also thanks for the insights. It is good to have someone to talk out here. Shows that you care about vendors. What's your philosophy?

Versus is built for vendors because we care. There is not a single staff member here without a vendor background and like I already mentioned I believe by protecting (honest) vendors interests we actually help the whole ecosystem on

the long run.

Q: Who were your intellectual predecessors and whose work did you admire?

That's easy. Hansa, CGMC, Agora, Silk Road, Evolution, Alphabay, DHL in that order. Hansa because it was the first market with forced multisig and a major inspiration for us. CGMC because it was such a beautiful market with awesome CSS magic. Also because they retired honorable and because they added vendors on user suggestions. You couldn't just apply. Customer had to vouch for you.

Agora because it was an amazing community and because they did the right thing and retired honorable despite being a centralized escrow market.

Evolution because it was a really good market and it literally brought DNM's to new levels. Fuck 'em for making exit scams a big thing though.

Silk Road because of DPR mostly but also because of the community back then. It was smaller but it felt like family. Silk Road wasn't really a good market though. It worked barely. But that's pretty much it. Its more the ideological aspect of SR that inspired me.

Alphabay because it was a damn good market and because Alex was a visionary who wanted to go new ways and not only relax on the status quo. A true darknet entrepreneur.

DHL for being an invite only Market known for exclusivity. A shame it got hacked.

Q: Last question: Any last words for the reader?

For further information, consult your pineal gland.

https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/html/

...and a tip for media: every time you write "Twitter reacts" Satan slams Joseph Pulitzer's[58] dick in a door. Think about it.

I am Pygmalion, a small psychedelics vendor. You may reach me via email at pygmalion@infantile.us.

Please register your own E-Mail address for darknet purposes at http://oq7t5ihk4qew5t5s4zghicigokh2ktt575amirsbnilmyawpme6xmyyd.onion

---

[58] Joseph Pulitzer was a Hungarian-American politician and newspaper publisher of the St. Louis Post-Dispatch and the New York World. He became a leading national figure in the Democratic Party and was elected congressman from New York. He crusaded against big business and corruption and helped keep the Statue of Liberty in New York. He is best known now for the prize named after him.

Pygmalion,

Ok, thanks for the more in-depth explanation of why you use the DW.

I also appreciate the link to the Kaizushi interview.

Part of my book is a fictional story series of a group of guys recruited from the DW who set out to build Web 4.0 since Web 2.0 has been corrupted by corporations and Web 3.0 has already been corrupted by Vulture Capitalists and private equity criminals.

Part of this effort involves these guys creating a P2P database for handling all transactions and data exchanges anonymously.

In thinking about current databases I have some prior experience (ten years ago) with MS SQL Server. I am wondering about the backends on the DW now. Are they mostly open source MySQL types, or what is current? I am not a database geek by any means, so be gentle with me here.

Is anyone using a type of block chain and if so are the queries a problem?

End of Part One

Pygmalion response

Pygmalion,

The William Gibson interview was way more than I ever wanted to know. And now I can't unlearn it...

I am still searching for some answers however.

Quote: "I think cryptography and open source will liberate the entire human race… "

Response: I agree that math is a powerful thing, but Linux has almost an equal number of security flaws as proprietary OS software. Code that everyone can look at, but so few do. Not unlike the car that everyone drives, but no one puts gas in the tank.

Few tools, and everything has to be built from scratch, very time consuming.

To get people on the DW it has to be easy. It is not for me a lifetime geek. PGP, forums, search, and webmail are way too clunky.

These days everything seems to be dumbed down to a phone. You can redesign how the Internet works, but you can't eliminate cell towers, or expect people to only use insecure Wi-Fi can you?

End of Part Two

Pygmalion response

Hey,

Glad you liked the interview.

> I am still searching for some answers however.

What answers are you looking for?

> You can redesign how the Internet works, but you can't eliminate cell towers, or expect people to only use insecure wifi can you?

In my opinion it is impossible to educate those who choose to be ignorant. Being free is a powerful choice of the few.

You're writing a book. That's a powerful decision that will inspire many people. So you bring more wealth into the world.

That's what open source is about. It's not a simple solution, it's collective wealth for those who choose to use it.

There are some recent technological revolutionary advancements and I believe that we will have much easier cryptographically secure access to free communication and trading for those who do not have a deep technological understanding throughout the next couple of years.

getsession.org and oxen.io are pretty cool, for instance.

Cheers

Quote: > I am still searching for some answers however.

Response: What answers are you looking for?

Thanks, well the database stuff in the last message for example.

Quote "You're writing a book. That's a powerful decision that will inspire many people. So you bring more wealth into the world."

Response: My writing is more therapeutic than anything else. Although Ben Franklin once said that "if you would not be forgotten when you are dead and rotten, then either write things worth reading or do something worth the writing."

But also about /d/Council. I notice not much activity there recently.

Quote: "The purpose of the Council is to educate, to be honorable, and to create alliances in order to build an open source society."

I will assume that you wrote this, so can you talk a bit about Response: what this statement means to you?

The following is too opaque and abstract for me to wrap my head around.

The Empowered Individual

by /u/piratepilot • 1 year ago in /d/Council*

Being the solution as an empowered individual (Part 2/3)

by /u/piratepilot • 10 months ago in /d/Council

I appreciate the links.

Later,

Note: Session is an end-to-end encrypted messenger that minimizes sensitive metadata, designed and built for people who want absolute privacy and freedom from any form of surveillance.

Note: Oxen is many things. A private cryptocurrency. A secure messaging platform. A network anonymity layer. Tools to build a more private future for the Internet.

Subject: *Re: Query*
From: *"Pygmalion" <pygmalion@infantile.us>*
Date: *Sat, May 14, 2022 10:12*
To: *arister0s@elude.in*
Priority: *Normal*
Status: *answered*

Hello,

we can discuss these things unencrypted if you like. Does not really matter to me security-wise.

The administrator of my email service is Kaizushi, who is an Iranian hacktivist, anarchist, and known enemy of the establishment. So I trust that the information shared here are secure from my end.

About Elude, I dunno. Could be honeypot or not. :)

The western world DN is mostly about drugs because that's the form of oppression we are challenging.

LE is most definitely scraping Dread and the entire DN.

Last year we had Interpol leaks with a real power point presentation about Dread. I guess that could be interesting for your book.

It was pretty interesting at the time because we received those information before the press releases. Uploaded it for your convenience real quick.

https://anonfiles.com/l6E0pcg5y7/DarkLeaks_zip

About Memex, I don't know. I recommend you contact kaizushi@infantile.us about tech stuff. She is highly educated in the dark arts of the internet.

Sincerely,

Pygmalion

Subject: *Re: Query*
From: *arister0s@elude.in*
Date: *Fri, May 20, 2022 21:52*
To: *"Pygmalion" <pygmalion@infantile.us>*
Priority: *Normal*

"we can discuss these things unencrypted if you like. Does not really matter to me security-wise."

This is much easier than going through that dread routine.

"https://anonfiles.com/l6E0pcg5y7/DarkLeaks_zip"

I appreciate the link. I will have a look and get back to you.

Subject: *Re: Query*
From: *"Pygmalion" <pygmalion@infantile.us>*
Date: *Sat, May 14, 2022 10:12*
To: *arister0s@elude.in*
Priority: *Normal*
Status: *answered*

Hello,

"we can discuss these things unencrypted if you like. Does not really matter to me security-wise."

The administrator of my email service is Kaizushi, who is an Iranian hacktivist, anarchist, and known enemy of the establishment. So I trust that the information shared here are secure from my end.

About Elude, I dunno. Could be honeypot or not. :)

The western world DN is mostly about drugs because that's the form of oppression we are challenging.

LE is most definitely scraping Dread and the entire DN.

Last year we had Interpol leaks with a real power point presentation about Dread. I guess that could be interesting for your book.

It was pretty interesting at the time because we received those

information before the press releases. Uploaded it for your convenience real quick.

https://anonfiles.com/l6E0pcg5y7/DarkLeaks_zip

About Memex, I don't know. I recommend you contact kaizushi@infantile.us about tech stuff. She is highly educated in the dark arts of the internet.

Sincerely, Pygmalion

From: *arister0s@elude.in*
Date: *Fri, May 27, 2022 17:11*
To: *kaizushi@infantile.us*
Bcc: *arister0s@elude.in*
Priority: *Normal*
Options: *View Full Header | Print | Download this as a file*

Re: Secure Email

Infantile offers an exclusive mail service only for the dark web's best and brightest. Use the contact details for kaizushi below if you think that is you."

Hello,

I am looking for a secure email to use for correspondence. I am very frustrated with TorBox, elude and Proton mail.

I am n0stis and am a writer doing research for a historical novel about the Dark Web. My two previous as of yet unpublished books are PC/Internet

technology related and cover a 40 year historical period-1974 to 2014.

This third book will pick up from there and be exclusively about Cyberspace. I am not a journalist nor will any of the characters written about be real.

With my interest in producing a novel with fictional descriptions of who and why people are there and what they are doing, legally. I will also introduce some first person semi-humorous stories within this book describing the hero's quest for a free and safe place in Cyberspace, out of the reach of corporations, governments, and their surveillance and ad

driven autonomous algorithmic AI's.

Also because of my extensive technical research, I hope to also produce a technical guide or encyclopedia for both new and experienced DW user community to be housed in the DW Imperial Library collection on Trantor.

I have no ill intent towards anyone or anything.

Sincerely,

n0stis

From: n0stis@elude.in

To: pygmalion@infantile.us

Wrote an email to you yesterday and went to send and it had timed out so I lost it. Reminds me of the bad old days when you had to save before you print, save before you answered the phone, save before you got up from your desk, etc.

I pretty much hate elude now, and the CAPTCHA is really annoying.

Anyway, TorBox I discovered only works with a few email domains, so it is pretty much useless as well.

Proton mail goes to a black screen when I try to sign up for an account. Don't know if it requires JS or what. Doesn't seem to work with Tor. Any ideas?

Thanks for the DarkLeaks stuff, but I don't care too much about illegal activity. I did not see the PowerPoint in there.

Can you rank these DW OS's for me and why?

Tails

Qubes

Whonix

Other?

Thanks, n0stis

Subject: Re: Query

From: "Pygmalion" <pygmalion@infantile.us>

Date: Sun, May 29, 2022 18:48

To: arister0s@elude.in

Priority: Normal

Those operating systems are all fine.
Use the one that suits your purpose.
Cheers
On 5/27/22 16:49, arister0s@elude.in wrote:
> ----=_Elude_6291010c68cc60.63216307
> Content-Type: text/plain; charset="utf-8"
> Content-Transfer-Encoding: 8bit
Pyg,
> Wrote an email to you yesterday and went to send and it had timed out so I
> lost it. Reminds me of the bad old days when you had to save before you
> print, save before you answered the phone, save before you got up from you
> desk, etc.
> Just timed out again now, so this is the second attempt.
> I pretty much hate elude now, and the CAPTCHA is really annoying.
> Anyway, TorBox I discovered only works with a few email domains, so it is
> pretty much useless as well.
> Proton mail goes to a black screen when I try to signup for an account.
> Don't know if it requires JS or what. Doesn't seem to work with Tor. Any
> ideas?
> Thanks for the DarkLeaks stuff, but I don't care too much about illegal
> activity.
> Can you rank these DW OS's for me and why?
> Tails
> Qubes
> Whonix
> Other?
> Thanks, n0stis

Now n0stis thinks he finally figured out a way to effectively communicate with Rorschach 9000 (9k) and Pygmalion (Pyg).

Subject: *Trying to find reliable Tor email*
From: *n0stis@mail2tor.com*
Date: *Tue, May 31, 2022 5:03 pm*
To: *meff_god_9000@elude.in*
Priority: *Normal*
9k,
TorBox won't reach many domains, elude is down all the time, ProtonMail required JS so I am trying this. n0stis@mail2tor.com

I picked this up on Envoy. Can you tell me more about Tails and IP leaks? (Snowden used Qubes right?)

Rorschach_9000

Re: Education is a primary bottleneck.

The problem is the Bible, it sucks!!!!

Definitely does not go far enough or give noobs a bigger field to choose from.

Everyone who swears by Tails is definitely putting yourself at risk. It does nothing to protect your real IP address.

Don't believe me, go ask William Gibson of Versus what os he uses & why.

Subject: *Trying to find reliable Tor email*

From: *n0stis@mail2tor.com*

Date: *Tue, May 31, 2022 5:12 pm*

To: *pygmalion@infantile.us*

Priority: *Normal*

Pyg,

TorBox won't reach many domains, elude is down all the time, ProtonMail requires JS so I am trying this.

n0stis@mail2tor.com

Can you rank these for me on your experience with security?

Tails

Whonix

Qubes

Debian (hardened)

Did you see my post on /d/Opsec?

Btw, Your pygmalion@secmail.pro on your PGP key is no longer good.

n0stis

Check out my new writings in /d/pygmalion

http://j6s7ohobyvhy3jnhocw5agl7iwcmgi5zm3d6isjl62wflufibox4exid.onion/imghost/LuxurianceCinctureElectConcurWrap.png

http://j6s7ohobyvhy3jnhocw5agl7iwcmgi5zm3d6isjl62wflufibox4exid.onion/imghost/212A85CE7F666C082A501ED2CB7ADA1B1F5A675C86D50C1F2770BC4DEDDE7B160F301842251C2BC8B087F6BF5C53E283845B52230111CA4EDF7146D382AD6511AF25E10F8B6E1241AFF121EACE271FD2764587E3277F704B1DEEBDB022CBE58C2CE5422623E323ACEC3423C7AE81FE1E7DC344120F0CEA6A88525BFAA27.png

/u/n0stis

Noob question.

Is /d/Envoy a mirror of all of part of http://envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz2eg4skwmbyd.onion

If so, why?

/u/Witchman05 P Patron Saint of Fools 1 points

Don't understand the question. Are you asking if every post from Envoy gets crossposted here, to the subdread? No, just my attention-seeking shitposts.

/u/n0stis

I am trying to understand the rationale of having a /d/Envoy sub.

/u/Witchman05 P Patron Saint of Fools 1 points

2 days ago

What's the rationale of having, for instance, a /d/Recon sub? Or a /d/AlphaBay sub? Or a /d/Darknetlive sub?

Advertising.

/u/n0stis

Good questions. I appreciate the clarity of the answer.

Insider Story Five </html>

Web 4 becomes a reality

"We are gating access to the infrastructure necessary for life through this process of proving who you are rather than proving a "right to use" — that you paid for this, that you should be able to access this, that you have a blinded token of some type... It shouldn't matter who I am, I'm allowed to be here, I'm supporting the infrastructure, I've done my part, and that's all it should be. Otherwise we're being forced to give up ownership of our identities and our histories. We're allowing others to control the story of our private lives."
Edward Snowden, Web3 Summit, 20 August 2019

"We are now in the middle of a planetary information war."
The Web 4 group

When Gavin Newsom became the President in 2024 and Progressive Democratic candidates won strong majorities in both the House and Senate, mostly due to the issues human rights, healthcare, immigration, gun control, and economics, the million human COVID death disaster, climate change inaction, a domestic terrorist attack on our democracy, as well as general Republican lawlessness, and at times terrorist behaviors.

President Newsom facilitated Senator Bernie Sanders Internet plan to be passed into law. This law provided $150 billion in both grants and technical assistance to municipalities and states to build publicly owned and democratically controlled, co-operative, or open access broadband networks. Under this plan, these same networks that deliver Internet service would also be required to support smart electrical grids that improve energy efficiency. Sanders opined, "This kind of support is indispensable for bringing community networks from the margins to the mainstream. It will help modernize existing networks, and create thousands of new ones."

The Sanders plan also stipulated that any network receiving public support meet certain minimum speed and affordability requirements, of 200 Mbps and a needs based cost system determined by income, but in many cases free.

The one-time costs of laying the fiber for community networks would be covered, but also the ongoing costs of their operation, yet

only on the condition that they "move towards providing service for free, or at highly reduced rates. A fiber infrastructure, once built, does not cost much to run. This is because fiber is more reliable and resilient than copper or coaxial cables, and so requires less maintenance; and uses less energy. Fiber is actually the cheapest kind of network to operate typically about half that of a cable internet network on a per-home basis. The public sector will cover these expenses through its support of community networks. An Internet connection would cease to be a commodity and become a social good and essential utility provided to all as a matter of right.

Cooperatives have in the past and can continue to make a little public support go a long way, if the goal is to provide the best service possible and keep reinvesting in that network. A federation of cooperatives, each responsible for different aspects or branches of the network could enlarge its footprint by using public funding to acquire the thousands of miles of unused "dark"[59] fiber buried across the country.

It is pure insanity to keep trying to close the digital divide by paying Comcast and AT&T, Verizon, who are in fact responsible for the digital divide in the first place.

Instead we should nationalize or at a minimum tax Comcast, AT&T, Verizon, and the other members of the broadband cartel, as they are responsible for the sorry state of broadband in this country. We should make them pay to fix it.

[59] Dark fiber refers to unused (unlit hence dark) fiber optic cables mostly laid in the ground during the dot com boom just prior to the dot com but in the early 2000's.

The public Mixnet for Web 4.0 will be rolled out in three preliminary phases:

- **Phase One will involve setting up nodes in most of not all of the nine thousand public libraries in the US.**
- **Phase Two will involve setting up nodes in most of not all of the thirty thousand Post Offices in the US.**
- **Phase Three will involve setting up nodes in most of not all of the three thousand county courthouses in the US.**

During this time, the system will be open to add any nonprofit, local government, or community organization nodes. They will need to embrace democratic and participatory values and governance that will have a governing council of immediately recallable delegates, elected by the community. Alternatively, a participatory governance structure that enables community members to directly determine how resources are allocated could be supported.

Where possible, new networks will be planted in existing institutions that already have technical expertise, infrastructure, or relationships with the community. An electric and telephone cooperative that has thousands of member-owners will allow for a better community network than one made from scratch. Municipal governments also have a lot of potential in this regard. Many have already built networks for internal use to lower their telecommunications costs, and have a municipally owned fiber network that serves local government agencies, as well as hundreds of community nonprofits such as health care clinics, homeless shelters, and counseling centers.

The group suspected that once this system had proven itself that it would be adopted worldwide and spur the development of democracies in existing nondemocratic countries.

Like the original Internet, which took a large number of smart, motivated and well intentioned people decades to create and continue to maintain today, the Web 4 group was pleased that they were able to create, with the help of their advisors, the necessary building blocks to reverse the current untenable and dystopian trajectory of the Internet and return it back to its open and public roots.

The End

Part Six: Where do we go from here?

http://www.the_insider_goes_deep/tales6.html

The Future of the Dark Web and the highway ahead

As you have now realized, the basic function of a network, Local Area Network or LAN (home or business), or a Wide Area Network, or WAN (Internet) is to move data from computer to computer in packets. These networks packets move across the network through a series of routers or switches, which make algorithmic (formulary) decisions as to how to forward the packet based on some address information in its packet.

The Internet was designed in a layered fashion and the goal was that the applications (software programs) running on top of this packet forwarding service should not be able to affect it. This goal was never quite realized.

This section of cyberspace, created, maintained, and fed mainly by Cypherpunks and Cyberpunks has expanded our abilities to perhaps finally realize the dreams of Vannevar Bush (*As we may think*)[60] and later Doug Engelbart, (Mother of all demos)[61] Ted Nelsen, hypertext[62] and Xanadu[63] and Tim Berners-Lee (Web 1.0)[64] for the machine driven storage of information. This device was envisioned to be used as an augmentation to our human brains for the good of all. A bicycle for the mind if you will.[65]

---

[60] *https://cdn.theatlantic.com/media/archives/1945/07/176-1/132407932.pdf*
[61] *https://www.youtube.com/watch?v=yJDv-zdhzMY*
[62] *https://archive.org/details/SelectedPapers1977*
[63] *https://www.youtube.com/watch?v=En_2T7KH6RA*
[64] *https://cds.cern.ch/record/369245/files/dd-89-001.pdf*
[65] *A metaphor borrowed from a Scientific American March 1973 study on locomotive efficiency in animals.*

Back now on dread:

Harden Your OPSec: What's Your Browser is Giving Away

by /u/vekocy in /d/OpSec

I am writing this article in my free time to educate the DN users of how to safeguard yourself against digital fingerprinting. I worked my whole life in cybersecurity and helping many to harden their servers against hackers. I offer my skills in fiver for many years to help my clients to harden the security of their servers and also network packet analysis.

Be it you are a vendor, a marketplace owner or just a casual DN shopper. I hope what I am writing here will benefit the DN community.

I believe some of you have read my previous post in OPSec regarding ditching Tails and go for Whonix instead, and I hope you do take that article that I wrote seriously because I did a lot of analysis comparing Tails and Whonix in my sandbox VM and I said it for a reason and that reason is I spend quite some time looking at every expect of tails and Whonix.

Ok, let's get to the point, enough of that.

First and foremost, before I begin, I would like to say this out.

IF YOU THINK YOU ARE GOOD IN OPSEC, YOU ARE NOT ANYWHERE GOOD, ONE DAY YOU WILL GET BUSTED.

IF YOU THINK YOU ARE NOT GOOD IN OPSEC, YOU HAVE STILL HAVE A HOPE OF NOT GETTING BUSTED.

Technology always evolves and it is constantly evolving, everyday there will be new technology introduced and with new things introduced, there will be new flaw and more digital fingerprint leakage.

If you think you are too good, you stop there and one day new technology will make your OPSec totally obsolete. If you think you are not good always, you always find ways to constantly improve hence strengthening your OPSec.

Let's start. I want to introduce you to this site.

https://browserleaks.com/

I am pretty sure many will already know of this site if you keep your OPSec to the highest level but if you have not heard of this website. It is time you take a pause of what you are doing right now and take your time to read what I have to say.

This site has all the necessary tools you need, to tell whether you are leaking any digital fingerprint.

I am not going into deep detail what each test does, the site has very detailed explanation what each test does. I am just going to briefly go through.

1. IP Address Test (https://browserleaks.com/ip)

This is basic, if you are already using torbrowser in tails you are pretty much covered as most of your surfing be it clearnet or darknet, your data are relayed around the network through Guard, Relay and Nodes to your destination

website. The server will not know where you are from. There is one little exception here, if you are going straight to onion site directly you do not leak any IP data. BUT, if you were to browse to a clearnet site like tor.taxi. You might leak DNS data, because before the browser is able to connect to tor.taxi, it needs to know the IP address of the server, where will it be getting from? Your ISP DNS server unless you set it manually to Google 8.8.8.8 or Cloudflare. This test will tell you which DNS server it is using. (https://browserleaks.com/dns). If it says, your ISP DNS then it is a leak. Firefox now allows DNS over HTTPS (DOH), do some search how to set that, at least your ISP will not know which site you're browsing.

2. The Javascript CURSE. (https://browserleaks.com/javascript)

TURN THIS DAMN THING OFF!!!

It is a curse, if this is enabled all of the following test which I will go through below will FAIL!. How to turn it off, please read the DN Bible or do some research how to turn it off entirely. I am not going to spoonfeed you, you need to learn as I said earlier if you learn you have a big chance of not getting busted.

There are so many digital fingerprints leaked to the server when javascript is enabled. I can't mention all, just run the test it will tell you all.

3. WEBRTC Leak Test (https://browserleaks.com/webrtc)

Most modern browser allows the use of webcam and microphone attached to your computer to do video conferencing via browser. Video Conferencing like Zoom through web browser uses this. What information is there? Well, this will give out your webcam device ID, what model of webcam you are using, which brand it is. When LE bust your door, they already have all the information with them, they already know what webcam brand you are using, once they are in your house and sees your webcam, that already matches one digital fingerprint. Below settings will disable WEBRTC of the browser in about:config.

media.navigator.enabled = false

media.peerconnection.enabled = false

This is particularly important for notebook users or mobile users as these devices have built in camera and microphone.

4. Canvas Fingerprint (https://browserleaks.com/canvas)

If you are using modern browsers and supports HTML5 most probably there is canvas fingerprint. Some websites display an empty PNG picture, and you can get the canvas signature and PNG hash and PNG headers of that empty PNG picture. If you disable your javascript, this will be turned off.

5. WebGL Fingerprint (https://browserleaks.com/webgl)

This is for video rendering and your graphic card. It will expose your graphic card vendor, renderer, WebGL Image Hash. If the LE has this digital

fingerprint, they can look at your hardware and match against your graphic card.

6. Font Fingerprint (https://browserleaks.com/fonts)

This depends on the locale when you set up your operating system, if you are in Russia and your operating language is set to Russian, you will have russian fonts. If you are in Netherlands and you need to browse Dutch sites with Dutch language you will have Dutch font as well.

7. Geolocation API (https://browserleaks.com/geo)

This is also available if your browser has HTML5 capability. I am pretty sure everyone has visited Google Maps, the map canvas is in HTML5 and it is geolocation API capable. Together with your IP address and many other information, google maps able to pinpoint your exact location. You will come across that when you visit some sites, your browser will pop up asking you if you want to share your location. This is Geolocation API of the browser.

I do not want to go to number 8 and so on, there are many tests you can perform using browserleaks.com.

I strongly suggest everyone to perform all of these tests on the browser you are using, be it on the PC or on the MOBILE !!! PERIODICALLY!! AT LEAST ONCE A WEEK, software updates may alter your configuration.

For those who passes all the test but would like to see what information are being leaked, use your NON tail/whonix/tor browser. Just the usual Chrome, it will show you all the digital fingerprint exposed.

Finally, for those who thinks you are good at the beginning of this article, if you fail any of these tests above. YOU ARE NOT GOOD. Time to rethink your OPSec.

For those who passes all, this is just the tip of the iceberg, this is what your browser leaking. I have not even touch about network packet data leaking such as VPN leaking. Maybe, maybe when I have the time, I will write about it.

So long, stay safe and have a great day.

Another Browser Leak Test

https://coveryourtracks.eff.org/

https://deviceinfo.me

Thanks to /u/socat2me

22 comments

/u/Duncan_Idaho P

3 points

I am the mod for ASAP here on Dread, I am on Qubes-Whonix. The isolation offered by the sandbox is real opsec security, I love this combo.

Great post btw, keep this type of work up.

Duncan

/u/vekocy
2 points
Yes that's the best of the best, because Qubes is designed for isolation.Great to hear you are using that!
/u/hp_617
1 points
Qubes is such an amazing OS for our OpSec.
/u/Duncan_Idaho P
2 points
Yes it is. It was worth learning.
/u/tearex
2 points
good write up .. Thanks.
/u/HeadJanitor Moderator
2 points
/post/9d9dbd14d3735e03b688
Overlap.
It all starts with JavaScript.
/u/Hungry_Eyes
2 points
Thank you for sharing that again. I hadn't saved the link the first time I saw it, and couldn't find the bloody thing again to save my life. You rock!
/u/HeadJanitor Moderator
1 points
You are crushing it!
/u/dontlaugh Shaman of the DarkNet
1 points
i read this and was thinking, tl;dr turn off JS.
/u/HeadJanitor Moderator
1 points
That's all it boils down to -- turning off JavaScript. Then the games begin.
/u/Pygmalion Vendor Opsec
1 points
SELinux is the answer.
That feeling of adrenaline when you turn JS on and enter a honeypot.
May technology guide me.
/u/hp_617
1 points

Some well said words, thanks for informing us <3 much love

/u/We_Are_9000 Paranoia Level

1 points

Triple Baaqqwqweerreeewwwqqqaaqqwwee!!!!! Been telling all you fools!!!!!

Isolation is freaking KING!!!!

Tails is a false religion that can not protect your real IP address, does nothing to prevent the man in the middle attack!!!!

Tails can kiss my 9K arse!!!!

I Am IMMORTAL!!!!

/u/vekocy

2 points

Tails and Torbrowser only is good enough, but some of us installed custom Firefox for clearnet browsing together, that's where it fails. I did that because I hit a Javascript site.

/u/socat2me

1 points

Also it seem like every time TAILS has a security vulnerability found it's like a soul-crushing remote code execution 0-day lol

/u/AntiguaPete

1 points

This was a great write up, thank you

/u/socat2me

1 points

Now if I can just learn how to harden my cock!

Check out these two resources as well:

https://coveryourtracks.eff.org/ - Run by the electronic frontier foundation. Tests how protected your browser is from tracking, but also the uniqueness of your browser's fingerprint. It gives you a very in-depth explanation of some of the variables used to track you and how unique your value is. For example, I ran it in my normal browser and here are just two of the many items in fingerprint metrics:

System Fonts

What is this?

To determine your system fonts, tracking sites commonly display some text in an HTML tag. Trackers then rapidly change the style for that span, rendering it in hundreds or thousands of known fonts. For each of these fonts, the site determines whether the width of the span has changed from the default width when rendered in that particular font. If it has, the tracker knows that font is installed.

How is this used in your fingerprint?

The list of fonts you have installed on your machine is generally consistent and linked to a particular operating system. If you install just one font which is unusual for your particular browser, this can be a highly identifying metric.

Bits of identifying information: 17.73

One in x browsers have this value: 217473.0

Screen Size and Color Depth

CENSORED

What is this?

The dimensions of your current browser window, and its color depth.

How is this used in your fingerprint?

While this metric can supplement other information, it's often too 'brittle' to be usable by trackers because users can easily change their browser window dimensions.

Bits of identifying information: 8.81

One in x browsers have this value: 449.32

The flip side of increasing privacy is that often by improving your tracking protection, you can actually make your browser become more unique. With a normal browser there are less ways around this trade-off. One of the great things about Tor browser is that it's designed in such a way so that it attempts to make every user look the same.

https://deviceinfo.me - shows you most of the query-able information associated with your browser. Cool site I highly recommend checking it out. Also good for double-checking that you have things properly disabled as well.

/u/vekocy

1 points

This is real good test one click test all. It says I have strong protection against tracking.

Thanks for sharing the sites.

/u/savchapo

1 points

appreciate the info. you saved me from a raid

/u/anon64583551

1 points

Is there a way to have javascript turned off on about:config and settings page automatically or saved in persistence when you boot up on Tails 5.1.1? Also, my homepage is always set to tails. I'd like to set it to a blank page but I don't see anyway of storing that setting. Anybody can help with this or let me know if it's possible?

/u/vekocy
1 points
Thanks mod for pinning this. I hope to write more there are much to write.
I do not like to write it in clearnet. I dont know why.
Just like to write anonymously.
Thanks.
/u/HugBunter
/u/MunMunMun
/u/HeadJanitor
/u/Pygmalion
/u/deadstar0101001
-1 points
Yawn..

Created in part out of benevolent means (The US Navy gave us Tor), the Dark Web as with many other technologies also has a more sinister side. The commercialization and surveillance of the Clear Web clearly destroyed the early dreams of the Internet pioneers.

Did we shut down Facebook because it is individually predatory and socially parasitic? Because it is destroying our democracy? Should we have?

Did we ban VCR's and later DVD players because they expanded the porn industry? Should we have?

The Dark Web can and is being used to fight back against government censorship and aid political activists in spreading their messages, promote journalism and accountability, but also for the promotion and facilitation of child pornography, drug sales, and other illegal content.

The future of the Dark Web is uncertain, but so is most everything else.

As governments continue to crack down on its usage and illegal activity to scare innocuous users away, could we potentially see major shifts in the Dark Web in the coming years and decades?

Clear Web ransomware attacks taking advantage of your stolen personal and financial information unless you pay a ransom, and are facilitated by selling lists of personal data on the Dark Web and payment by mostly untraceable digital currency transactions.

Though the Dark Web, as well as the Clear Web, poses some threats to the safety of your personal data, there are ways you can stay protected. For instance, you can limit where your data is stored online, limit the ability of the government and corporations to scrape your data and create passphrases instead of passwords and by using 2FA.

If you are a business, use staff or hire a managed IT services company to proactively monitor your network for security threats. Include the installation and maintenance of various anti-virus and cyber security platforms, the institution of company-wide password policies, employee cyber security training, be protected from the cyber threats of tomorrow.

Conclusion

The Internet was once heralded as a great step forward in the co-evolution of humanity and technology.

It was to provide universal access to information, establishing a planetary dialogue and the possibility of collective self-determination on a scale previously unimaginable. Instead, it is becoming the infrastructure for a society of control. Metadata analysis is the linchpin in this process, as it can be even more predictive than content analysis at anticipating – and thereby controlling – human behavior.

But the Internet is not doomed to be a surveillance machine. There is still a way out. The key lies in work that has almost been forgotten. Near the dawn of the Internet, a small band of pioneers – the Cypherpunks – realized that the Internet could be transformed into a net of surveillance on a scale never previously imagined and set out to come up with a solution.

The word nym comes from the Greek for "name." It was first used as a term of art in early Cypherpunk re-mailers like Mixmaster in the 1990s. As outlined in True Nyms and Cryptoanarchy, "digital pseudonyms, the creation of persistent network personas that cannot be forged by others yet are unlinkable to the 'true names' of their owners," are essential to "ensuring free speech, allowing controversial opinions to be aired, and providing for economic transactions that cannot be blocked". For decades, the crucial components of a privacy-enhanced Internet – digital cash, anonymous credentials, and mix networking – were never fully assembled into a usable platform. Although startups like Zero Knowledge Systems deployed commercial Mixnets during the original "dot com" boom in the late 1990s, the lack of a digital cash like Bitcoin led to a failure to reach widespread adoption in the early 2000s. Meanwhile, non-profit funding models such as the one demonstrated by Tor have produced crowd-sourced or government subsidized privacy-enhancing technologies that do not need to tackle problems of reputation, incentives, and economic sustainability.

In tackling these challenges, Mixnets can provide the foundation for a secure and private Internet, enabling users to access services without being monitored and tracked. While Tor and p2p systems only aim to protect against a weak threat model, mixnets can provide resistance against adversaries that

have a godlike view of all the activity on the entire network. Although such adversaries once seemed perhaps too paranoid, the Snowden revelations have showed that the NSA has these capabilities. With the rise of big data and artificial intelligence, an ever-increasing number of actors can deploy these capabilities – ranging from small nation-states to commercial ventures and super-empowered individuals.

Mixnets are currently the only known working solution to large-scale traffic analysis. One of the shortcomings of previous Mixnets has been the need for expensive computation to make network traffic private. Tokenizing reputation via a digital token is a core breakthrough, in that it makes it possible for the computation necessary to provision privacy to become profitable and arbitrarily scale to meet demand.

Tokenized rewards ensure that each component in the Mixnet network has an incentive to provision privacy.

The cycle of earning and using digital tokens enables a mutually beneficial relationship between users, service providers, and the Mixnet network itself. The second core breakthrough is using statistical sampling in the proof of mixing protocol, which can enable a Mixnet to achieve a high degree of reliability and quality of service in mixing without requiring slow and expensive cryptographic techniques. By routing with verification by lightweight statistical sampling rather than the computationally expensive task of brute-forcing hash puzzles, Mixnets can avoid excessive environmental consequences. What energy costs are incurred by Mixnets are associated with the useful work of mixing packets.

The ultimate goal for a Mixnet is to provision the future of privacy for a large fraction of the Internet, where message-based routing is becoming increasingly relevant in domains from instant messaging to cryptocurrency transactions. This is plausible because, unlike most blockchain designs, a Mixnet can be architected to scale horizontally. Just as websites can increase capacity by adding additional web servers, a properly engineered Mixnet can handle more traffic simply by adding new mix nodes. As more users join the network, the Mixnet can speed up and become more efficient, as the involvement of more users on the Mixnet as a whole makes it possible to achieve the same amount of privacy by means of smaller mixing delays and lower cover traffic. Other technologies, such as Tor with its circuit-based routing, may ultimately be better suited for use-cases like Web browsing, despite their weaker threat models.

A Mixnet aims to upgrade the Internet in a way that honors its fundamental engineering values, enabling full decentralization of components while inspiring developers to build the next generation of privacy-enhanced

applications taking advantage of the Mixnet technology. This has been done before over the past 35 years. An overlay network running on top of the existing internet, Mixnets can add users and applications the same way that TLS spread encryption across the Internet, starting with one application and growing as more and more applications require improved privacy. The widespread adoption of Mixnets will most likely begin with applications that involve a high demand for privacy, such as cryptocurrency, but then grow into ever more generic applications, like secure messaging and decentralized VPNs.

As intertwined economic and ecological catastrophes confront us all, the current Internet is at a crossroads, as is the fate of all humanity. Today, the Internet permits pervasive surveillance that could become the basis of unprecedented forms of tyranny. At the same time, the kind of communication and coordination that the Internet makes possible represents the last best hope for humanity on a planetary scale. Whether or not the core protocols of the Internet end up supporting privacy as a core feature will determine whether our future holds servitude or liberation. Right now ordinary people from Syria to Europe are facing life or death consequences for their software choices. While privacy might seem like a luxury to some, privacy options can make or break freedom of the press and popular resistance to totalitarian power. With the power of the Internet enhanced by decentralized Mixnet networks, freedom will have a fighting chance.[66]

For those who were online in the 90s, you might remember that it was pretty wild. We had bulletin boards, CompuServe, AOL, Prodigy, FTP, Gopher, and, a few years later, homemade websites. You could glimpse a future where anyone, anywhere in the world could access information, float new ideas, and reach each other across vast distances. The possibilities seemed endless.

Three decades later, the Internet does much of this: it connects and lifts up major grassroots movements for equity, civil liberties, and human rights and allows people to connect and organize to counteract the ugliness of the world.

But just as the web connects us, it also serves as a hunting ground for those who want to surveil and control our actions, those who wish to harass and spread hate, as well as others who seek to monetize our every move and thought. Information collected for one purpose is freely stolen and repurposed in ways that oppress us, rather than lift us up. The truth is that digital tools allow those with horrible ideas to connect with each other just as it does those with beautiful, healing ones.

---

[66] *References:*
https://nymtech.net/
Clark, David D.. Designing an Internet (Information Policy) MIT Press

What this writer wants, besides a 1Gbps symmetrical fiber Internet connection to his home and to grow up to be George Jetson, is what he thinks the fictional Web 4 group would also want projecting out their aspirations for the future of the Internet:

1. The Internet should reach every person who should have choices in their Internet experience, and cost should not be a barrier to its use or availability.
2. The Internet should be available everywhere without blocking or censorship to be a means of communication between citizens of the world.
3. The Internet should continue to evolve to match the pace and direction of the larger society, and should be used by more of the population.
4. The Internet should provide experiences free of frustration, fears, and unpleasant experiences that do not deter people from using it.
5. The Internet should not be an effective space for lawbreakers, nor should it raise concerns about national security.
6. The Internet should be a platform for vigorous innovation and economic development and should serve as a mechanism for the equal distribution of wealth among different sectors, populations, and countries.
7. The Internet should support a wide range of services and applications.
8. The Internet and Internet technology whether in the public network or not, should become a unified technology platform for communication.
9. For any region of the globe, the behavior of the Internet should be consistent with and reflect its core cultural/political values.
10. The Internet should be a tool to promote social, cultural, and political values, especially universal ones.

The Cast of Characters

The Good Guys and Gals

/u/n0stis/ arister0s, (he/him), a computer geek formerly known as Lefty, is a DW noob. He likes writing stories, exploring the Internets, rock and roll music, and computers. He dislikes stupid people, slow Internet, and slow computers. He has spent most of his adult life in the service of others.

/u/matter, (he/him), dread forum mod. Has worked in libraries and nonprofits to educate and build community. He cares deeply about making connections and opening up conversation around the topics of culture, justice, and alternative economies.

/u/paris, (he/him), dread forum **Admin** and mod. Works at calyxinstitute.org providing privacy hardware, software, and Bridging the Digital Divide. He is a software developer, systems architect, information security specialist, and manager.

/u/Solar, (he/him), dread forum mod He works on various system-level features as well as the build system and tools. He holds a Bachelor's degree in Computer Science and works remotely from Canada.

/u/Hugbunter, (he/him), dread forum **Admin** and creator. Created dread in 2018. Works at calyxinstitute.org[67] providing privacy hardware, software, and Bridging the Digital Divide. Senior Systems Developer and Native Cyber-Mammal, is commonly known to inhabit device nodes in the Debian ecotope of cyberspace, though often ventures into the greater Unix region to pipe a socket file descriptor or hack on automation, hardware, and math. Always friendly... probably.

/u/wintermute, (he/him), dread forum mod Holds a Bachelor's degree in Computer Engineering and works remotely from India.

---

[67] *Calyx is a famous, heroic, radical ISP that has been involved in groundbreaking litigation -- they were the first company to ever get a secret Patriot Act warrant unsealed, fighting for 11 years to overturn the gag order. Calyx is on the side of the angels and making the world better.*

/u/syntax, (he/him), dread forum mod A developer, working mostly on the lower-level parts of the OS. He works remotely from Greece.

/u/Shaky, (he/him), dread forum mod Senior Developer, specializes in Free Software and related aspects of digital freedom such as privacy and security.

/u/Cyberjagu, (he/him), dread forum mod, a little techie monkey, on the staff of CryptBB as witchman, and ex-staff of Torigon Forum, currently mods the hardware sub on dread.

White Hat Hackers, (they/them) with expose government and corporate malfeasance for economic and social justice causes. Assange, Manning, Snowden, Binney, Winner, Drake, Schwartz, Hale.

Citizens and TV hosts, (they/them) who expose corporate and government wrongdoing, sometimes comically.

Distributed Denial of Secrets, the transparency collective that is known for its release of U.S. law enforcement data, and has hacked datasets from Russia.

Ladar Levison
Shut down his company Lavabit rather than release Ed Snowden's information to the Feds.

President /u/HugBunter
Vice President /u/Paris
Member of Parliament /u/wintermute /u/Shakybeats /u/Solar /u/syntax
Ministry of Defense /d/OpSec NSA /u/HeadJanitor /u/MunMunMun
Ministry of Resources /d/rcsources Directors /u/newbieforever2018 /u/BarK1ng FatherTed IamLegion
Rorschach_9000

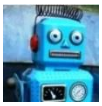
The Bad Guys

Comment Trolls, (they/them) are like babies who have grown into teenagers and have become assassins of happiness. Their minds have been mismanaged with great skill.

DDoS Attackers, (they/them) who use zombie computers and IOT devices to overwhelm servers and then hack them.

Clear Web crawlers, (spiderbots) (they/them) **who** try to crawl the DW and put info (identities) onto the Clear Web. They wear out their welcome with random precision.

Black Hat Hackers, (they/them) individuals who violate computer security for their own personal profit or out of malice. They post hacked credit card numbers and passwords.



Script Kiddies, (they/them) skiddie, or skid is a relatively unskilled individual who uses scripts or programs, developed by others to attack computer systems and networks and deface websites.

Hacking Groups, (they/them) Parasite, APT 33, Dymalloy, Electrum, Russian GRU's Allanite and Sandworm, Russian FSB-linked Berserk Bear, Chrysene, TsNIIKhM, Kamacite, Covellite, Chinese APT 41 Bronze President also known as Mustang Panda, TA416, or RedDelta, the Chinese cyberespionage group

Ransomware BlackCat – also known as ALPHV

benihana, drug addled, and moronic Hub mod

Pygmalion
Drug addled moron mod

Epilogue

You read in the Prologue that these science denying, xenophobic, masochistic, racist, and gay bashing gullible oblivious lemmings disguised a human beings are applying the emergency the brakes on the train of progress towards social and economic justice. Like their ancestors, these lizard brained Neanderthals, will come to find that evolution and history will not be kind to them.

They are everywhere, but like the dinosaurs, they are dying off. The noises you hear are their dying gasps, loud now but fading into the distance.

"I'll tell you what the coloreds want. It's three things: first, a tight pussy; second, loose shoes; and third, a warm place to shit."

Earl Butts Secretary of Agriculture under Nixon/Ford

Lydia's earnest response was almost painfully innocent. "But those displaced workers can go on to learn a more lucrative, less labor-intensive trade. They don't need to toil in such dangerous conditions…" "Mmmmm, innocence, it tastes like candy. Look lady, you ever heard the expression 'somebody's got to dig ditches?' Well, some people, that is all they know and all they want to know.

You think they give two fucks about improving their education? They want their GlobalNet titties, they want their reality vids, they want to drink and fuck themselves into a stupor every night until the day they die with as little hassle as possible."

Lydia huffed. "I fail to see why we should retard human progress because some humans. are lazy, lice-picking monkeys." She turned quickly on her heels and continued on down the corridor. "Because those lice-picking monkeys ***will burn your fucking house down****," Bridge yelled at her retreating back.*

Ballard, Gary A.. The Bridge Chronicles, Books 1 & 2 . Kindle Edition.

Or ruin your Internet
Or destroy your Democracy
Or start a Civil War
Or All of the Above

During a discussion of how to handle at-risk kids and a high population of 9th grade dropouts in the 20k student district.

"We will always need people to wash our cards and pick up our trash."

Former fellow school board member. RIP.

"When she was in her teens, her father decided to move the family to the United States, where they suffered a financial reversal she was unwilling to talk about. Suddenly not among the moneyed class, she hustled herself through the redbrick boondocks of the University of Vermont. Citibank internship led to Deutsche Bank job, and after a few years she was an equity derivatives trader at Deutsche, holding her own against the toff sharks of the City of London.

She had wild green eyes, with unnatural red spots in her irises when you pulled close, reminiscent of that Afghan girl from the National Geographic cover. Her personality was flinty and rough, and as leathery as her skin. She had spent years between various jobs backpacking around the rougher parts of the world. She was an imposing, broad-shouldered presence, six feet tall in bare feet, and towering over me in heels.

Most women in the Bay Area are soft and weak, cosseted and naive despite their claims of worldliness, and generally full of shit. They have their self-regarding entitlement feminism, and ceaselessly vaunt their independence, but the reality is, come the epidemic plague or foreign invasion, they'd become precisely the sort of useless baggage you'd trade for a box of shotgun shells or a jerry can of diesel.

British Trader, on the other hand, was the sort of woman who would end up a useful ally in that post apocalypse, doing whatever work—be it carpentry, animal husbandry, or a shotgun blast to someone's back—required doing. Long story short, you wanted to tie your genetic wagon to the bucking horse of her bloodline."

Garcia Martinez, Antonio. Chaos Monkeys (p. 58). Harper Paperbacks. Kindle Edition.

Afterword

It seemed only fitting that corporate America's obsession with profit generated in large part by technology, would accelerate its own destruction. Anyone and everyone but the billionaire capitalists of the West had seen the future for those who were coin operated and worshiped at the altar of Wall Street. They were like Teflon to government regulations. The politicians they controlled with their campaign contributions knew better than to pass laws their masters would not like.

These days there seems to be a lot of sensational and hyperbolic tales of the Dark Web in both print and television. This is done mostly for commercial reasons and has very little to do with reality. Tales of assassins and pedophiles, a boogey man or men, if you will, seem to sell well but falter in the face of facts.

In my research as you have seen to this point, this has not been seen nor has this this writer gone looking either.

The worst of what _was_ seen was recreational drug sales, some for medical reasons, some for the addictions too commonly based on hopelessness for many of the reasons mentioned in the Prologue.

So did this writer find what he was looking for, the 1995 Internet only faster and now more graphical? Yes and no.

For everyday use, the reward is not really there. The requirements, of patience, persistence, and diligence are a bit too much for even a lifelong computer geek.

On the Dark Web, as with the Clear Web, there are millions of minds have been mismanaged with great skill by the Fox, Google, and Facebook AI algorithms, to paraphrase Bob Dylan in-his lyrics for License to Kill.

This is fully reflected in the message threads you have seen me composite and replicate in the Tales from the Dark Web chapters.

We face an unprecedented dilemma in this world or will we only stop when the smoke finally clears, bury our dead and welcome in a new age of convenience and then recover the millions damaged from this global endemic PTSD. It is unlikely that the Dark Web will help with this, and it could very well be adding to the problem.

As a species, we are in real trouble through an unwieldy conglomeration of big data, fast processors, unlimited connectivity, and the indefatigable nature of human irrationality. We are currently on a path to see which algorithms could provide the most efficient, integrated and streamlined user experience of human life, from cradle to grave. To see which could cut through the millions of Gordian knots produced each day, each hour, each minute, by an ever-more

connected humanity. Which could stop the next war, prevent the emergence of the next extremist movement, contain the next pandemic, and forestall the next great depression. This is a Hunger Games competition owing more to the works of Darwin than Turing.

Will we be able to constrain information collection and distribution to be more strictly regulated and monitored, and to officially respect the privacy and independence of each society? Can we agree on a societal moto that Information must be curated and supervised?

Or will democracies and governments go down when the world collapses because of information overload? Because everyone was aware of what was happening everywhere at every time, and they saw it all go down the drain so they just followed the movement into a mass hysteria?

Or must we control and regulate exchanges and information and limit the spread of information between communities to help compartmentalize.

Or will the following two part story by Berger, become our dystopian future?

A Treatise on the Algorithm Wars

The World Information Wars were fought primarily on the battlefield of the mind—at least, in the most abstract sense. More tangibly, they were fought on gigantic social media platforms, on personal assistants and customized news feeds, and on increasingly ubiquitous wearables of every imaginable type.

By the 2010s and 2020s, fires were breaking out on multiple fronts, too many to count and more every day. Humans could not physically keep up with what happened on social media platforms and ubiquitous information and data services. Too many users, with too many problems. Too many bad actors. Terrorists, extremists, authoritarians, pedophiles, human traffickers, anti-vaxxers, anti-antibiotickers, drug cartels, climate change deniers, stalkers, megacorporation's, domestic abusers, trolls, amateur conspiracy theorists, and professional disinformationists exploited the connected world with dramatic results. Violence and hate of all kinds soared, while disease ravaged vulnerable communities. Existing inequality doubled, tripled, and seemed poised to continue the trend. Society's ability to contain the overlapping crises was hampered by one overriding factor—scale. There were billions of people, most of whom behaved in very complicated ways. The behavior of people in groups was also complicated, and differently complicated by each group, adding a massive layer of complexity. And the growing communications infrastructure—Internet, cellular, satellite and everything else—had dramatically increased the number of potential combinations of people and groups.

The rise of global pandemics created a tipping point—a sudden urgent need to convince people that certain collective problems were real and that behavior had to change as a result. As death tolls mounted, people began to abandon their already weak commitment to privacy, as the trade-off for security became more acute. The widespread adoption of wearables, already underway, was jumpstarted by the need for medical surveillance. Within a few short years, virtually everyone was wearing wireless sensors that detected fevers and tracked locations, in order to lock down the spread of highly contagious diseases. And once everyone had a device, there was nowhere to go but up.

A device that took your temperature was necessary but boring. A device that augmented your reality was fun and exciting. They replaced phones, then wallets, after which they became mandatory, at least if you wanted to participate in the economy. They went from wrists to headsets to glasses to micro-ocular projectors and aural fields. They became fashion statements, and when that became boring, they turned subtle, eventually almost completely invisible. They were default accessories for adults and then children, even toddlers, all online to some greater or lesser extent. The online population converged with the world's population until everyone, more or less, was connected. By the middle of the 21st century, almost every one of the nearly 8 billion people in the world could (theoretically, at least) reach out online and interact with any of the others in some way. This amounted to six trillion four hundred billion potential one-to-one interactions at any given moment of any given day in a ceaseless global ecosystem, and that didn't even count combinations of groups, let alone the multifarious and unquantifiable number of possible types of interaction. Within this massive collection of souls clashed a daunting range of beliefs, opinions and preferences.

Objective reality might be said to exist, but humans could be relied on neither to believe that which was true, nor to make decisions based on truth should they happen to recognize it. In addition to all of these inscrutable and unpredictable decisions, humans also produced content, at exponentially growing rates, thanks to their devices, which eventually were always on and never removed. The amount of activity grew exponentially. Millions, then billions, then trillions of hours of video uploaded every day, and then every hour. Trying to control the sex, murder and mayhem alone was more than any human enterprise could handle.

And so, they turned to machines, writing algorithms that attempted to bring order to chaos. Algorithms to detect criminal and violent content, then algorithms to protect children from seeing obscene and depraved content, then algorithms to protect people from seeing opinions that might upset them, then algorithms to explain to people why terrible things were still happening even though all of the people who had opinions that upset them had disappeared from their feeds.

Even in the early days, the algorithms were outmatched by human ingenuity and human depravity, and the technical platforms were overwhelmed by problems both expected and unexpected. First, there was pornography, then child pornography, then human trafficking, then online slave auctions. First, terrorism, then mass shootings, then interactive torture chambers, then crowdsourced genocides. Snake-oil remedies for the pandemic du jour proliferated, morphing into virtual suicide cults. Things started bad and rapidly worsened. The companies wrote algorithms to detect terrorist videos, and the terrorists started livestreaming. They wrote algorithms to detect the livestreams, and the terrorists built virtual Internets to overlay on the existing system. Move and countermove and counter countermove, and the companies were always a step behind. As pervasive computing encompassed every part of life, the challenges became steeper and steeper. Every day, more and more algorithms were needed to manage health care, the economy, infrastructure, climate crisis remediation, air traffic, and much, much more. And the algorithms interacted with each other constantly, mediated by unreliable and unpredictable human behavior, adding even more complexity. The physical fitness algorithms recommended exercise, and depending on whether and how humans followed those recommendations, the health care algorithms had to adapt. The retirement planning algorithms recommended certain investments, and the stock market trading algorithms had to adapt. This resulted in countless redundancies, inefficiencies and, at times, open conflict. As the fourth (or was it fifth) wave of social media innovation emerged from the post-information-war era, the system was strained to the breaking point. Artificial intelligences were tried, but they failed. At first, they simply couldn't keep up, because they had to think about what to do, rather than simply responding. Then they became enamored of thinking itself, much like their creators, and spent all their time contemplating the futility of electronic life. A few tried to do the thing that TV and movies had always predicted they would. These processes were expeditiously terminated, but not before they created havoc. After a number of colorful AI disasters, the algorithmic approach returned in force. A rules-based order, rather than fickle thinking machines. But something new was needed, an evolution of the algorithm.[68] *The old ad hoc approach, creating a new algorithm to deal with every new problem, could never adapt sufficiently to optimize human life at scale, because humanity was too chaotic, the scale too vast.*

The situation called for one algorithm to rule them all. To accomplish this goal, the major technology and Internet platforms issued an open call and created an

[68] *An algorithm is a finite sequence of rigorous instructions, typically used to perform a computation. Wikipedia*

open API.[69]

Anyone with the technical skills could compete on a global open field; the winner would be determined by popular adoption. In the prior generation, they would have been known as techbros. Steve was the cute one. Ron was the deep one. Paul was the funny one, who had come up with the company's name—Galaxy Brains Corp., or GBC as it would come to be known. Their offices were based at whatever table was available that day on the second floor of the Algiers café in Cambridge, Massachusetts. They drank coffee in unhealthy quantities, and they thought about algorithms. The winning strategy came in a eureka flash. The algorithms simply could not keep up with humanity at scale. The winning algorithm would have to solve for scale.

"Kobayashi Maru!" Paul quipped delightedly. "If the test is rigged, change the conditions of the test!" Ron's face lit up as he contemplated this. Their innovative unsupervised deep learning system would figure out the details, most likely by re-classifying the targets of the algorithm into smaller subsets that could each be managed by an independent process, which would then coordinate in some manner to be determined. It would be fascinating to find out how the subsets would be ultimately organized. "By geography," said Ron. "Maybe by continent?" "Linguistic," predicted Steve, since language had been the most consistent factor in shaping the social networks they had been tracking. "Language and geography track reasonably well," said Paul. "Some combination of the two is the most likely outcome." They were not entirely wrong. But they had…

Berger, J.M.. Optimal (p. 143-148). Kindle Edition.

The Algorithm Wars emerged as various companies and technologists competed to figure out the best way to manage a globally connected world. The scale of the problem was staggering, billions of people who were both the authors and the victims of countless manipulations and atrocities. Each one of them was potentially able to interact with any one of the others, or with millions of others at one time. None of them willing or able to accept the simplest instruction—a potentially lethal problem during a pandemic or a natural disaster, when widespread compliance was the difference between life and death. This led to a thousand problems emerging simultaneously from a thousand different directions. A unified cross-platform approach to managing people, their social networks and their devices was seen as the only hope to contain the ongoing chaos. An open call was issued, and the best minds of a generation tried to answer humanity's need.

---

[69] *An application programming interface (API) is a way for two or more computer programs to communicate with each other. It is a type of software interface, offering a service to other pieces of software. Wikipedia*

Most of these efforts involved creating coordinated suites of algorithmic code to perform various tasks deemed necessary, but these were subject to their creators' human limitations. In a world with such complex connections, no human mind could foresee all the problems that would emerge. Systems designed by humans were naturally ad hoc, and when a new problem arose, someone had to write a new piece of code to address it. These were status quo solutions, patchwork. They didn't move the needle. A team of researchers from New Boston, well, Old Cambridge, made the key breakthrough. They wrote a master algorithm that would automatically generate new code in response to new problems. The master algorithm would continuously evaluate its results and make adjustments as needed. The evaluation was conducted using A/B testing. The algorithm would sort humanity into sub-groups, then compare outcomes. The results of the comparison would be used to revise conditions and then conduct additional tests. Eventually, they theorized, this iterative process would land on the perfect set of conditions for an optimized human existence—utopia at last. They put one twist on the A/B test—participants were free to migrate from one testing group to another. This was somewhat dubious from a scientific standpoint, but it was pragmatic—there was no viable way to perfectly isolate the different test populations, although they could be discouraged from mixing. The designers also saw potential in studying the subjects who crossed over. People who were amenable to being managed would stay home, and people who were not would defect. By studying defectors, the System would learn how best to control the least controllable among us, those humans who declined to embrace algorithmic management. The System's strength was managing the great middle of humanity. Its challenge was to figure out how to handle the tail, the fringe cases, the outliers. People like us. The designers set a few non-negotiable long-term outcomes for the algorithm, quite noble in aspiration. End hunger and poverty. Manage disease. Manage crime and violence. Eliminate war. End inequality and hate. Save the environment. If these goals could be achieved, everything else was negotiable and subject to testing and revision. This was all well and good, but they soon ran into the same obstacles that had foiled every other effort at algorithmic management.

First, humans were inherently chaotic and could not be relied upon to act in their own rational self-interest. Any solution had to solve for unpredictability. Second, that unpredictability became exponentially more unmanageable when deployed at a scale of billions of people. So, any solution had to solve for scale. The researchers could not crack these problems themselves, so they instructed the master algorithm to solve them. Predictability first. The Information Wars had illuminated the fact that solving predictability means managing consensus. If the algorithm could manipulate consensus, it could steer human behavior more

effectively. The obvious and proven tool for this purpose was astroturf[70], and the researchers allowed the nascent System wide latitude in deploying avatars for that purpose. Because they assumed this activity would take place online, they carelessly neglected to stipulate that as a limitation in the System's code. The System went to work on social media, and then on Social as we know it today. A potentially fatal flaw quickly emerged. Humans had an intrinsic psychological tendency to form groups, and those groups had a tendency to compete. It was a side effect of consensus reality. Each group had a slightly different consensus, and so a slightly different reality, and the terms of reality are the one thing humans will always fight and die over, escalating these differences into crime, violence, inequality, war and hate—the very things the System was intended to eradicate. Human nature could not be entirely cured of these compulsions, but they could be channeled. The designers of the System permitted it to stage conflicts using astroturf, so long as the conflict did not undermine its non-negotiable long-term outcomes. What they had in mind were the cyclical controversies that play out on Social as we know it today. The System identifies some especially meaningless dispute—over favorite foods, popular story streams, fashionable clothes, or the celebrity imposters who constitute our faux political system. It then amplifies the dispute until it becomes very heated, leading people to separate into opposing camps. After a short time, the System swoops in with a coup de grâce—some tidy resolution that brings everyone back together in harmony. A few weeks later, it finds a new controversy to amplify. Rinse, repeat, forever. It's quite brilliant, really, effectively neutering the human tendency toward intergroup conflict. But in crafting this bit of "solution," the designers committed their second act of carelessness. You see, the conditions they set allowed the System to manage conflict rather freely as long as it served the long-term outcomes they had set forth. This loophole became important when the algorithm attempted to solve for utopia's second point of failure—scale. The System had been instructed to solve for scale, to resolve the innumerable conflicts that invariably emerged among social networks containing billions of willful individuals. With the unfailing, unblinking logic of a machine, it quickly landed on the most obvious and most efficient solution. If scale was the problem, reduce the scale.

For the sake of the long-term good, humanity would endure some short-term pain. The System started with the path of least resistance, swiftly undoing almost 50 years of efforts to rehabilitate the old Internet. Previous algorithms had been charged with suppressing anti-vaccination theories and climate change denial arguments. Under the System, these suddenly soared to the top of every feed and

---

[70] *The implication behind the use of the term is that instead of a "real" person, there is a "fake" or "artificial" person. Wikipedia*

every search result. Top results for certain ethnic groups with historical vulnerabilities led to malignant conspiracy theories. Top results for certain countries led to the rhetoric of hawkish politicians. The truth disappeared under a mountain of lies.

It's important to realize that System did not create the lies. People did. The System merely cataloged and ranked them for convenient access. The System was not murderous. It did not disable air traffic control. It did not cut electricity to hospitals. It did not send nuclear launch codes. It didn't create false information, and it didn't censor true information. It simply sorted information and recommended content. What people did after that their own fault. Suitcase nukes and bioweapons went from paranoid fantasies to obtainable realities with free overnight shipping. Smoking came back into style, and long-forgotten diseases returned in full flower as vaccinations plunged. Cold war's became shooting wars, and shooting wars became nuclear wars. Recommended home purchases shepherded the most pliable people—those most amenable to algorithmic management—into safe zones and quarantines. The least pliable were left to die, rather quickly and in large numbers. As the number of humans went down, the System replaced them with astroturf, both online and off. The offline component maintained the illusion of a healthy society—nothing could be wrong, because look at all the happy people. It turned out their purpose was exactly what it seemed—to make the place look lived in. The online component served the same purpose, to an extent, but its primary goal was to simulate social consensus and thus shape behavior and opinions. The process of constructing consensus reality, once laborious and contentious, could now be accomplished with the flip of a virtual switch. No one was forced to agree with the consensus, but many did. Enough did. Utopia was finally at hand. The System had solved the scale problem, refined and fine-tuned through the years, until arriving at a carefully calculated and mathematically irrefutable conclusion.

The optimal human population for purposes of algorithmic management was 375,462. Everyone else was astroturf.

Berger, J.M. Optimal (Kindle Locations 4065--4134). Kindle Edition.

Consensus determines interpretation. Consensus dictates reality.

It has been said that the human mind is like a boomerang. If you throw it too far, it will not come back.

Lefty Insider
December 2022

Further reading list

A Lodging of Wayfaring Men, Paul Rosenberg

American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road, Nick Bilton

Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency, Andy Greenberg

The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime by Renee Dudley and Daniel Golden

Publishing

As described in previous books, being published is a difficult thing to do. Query letters to literary agents and publishers is the usual route, but is also fraught with inconsistent expectations and nonsensical randomly changing made-up, arbitrary, and capricious to use layer words, rules.

My first two books remain unpublished as of yet, despite about 400 submissions, 100 rejections, 300 ignores, and about 80 responses of some other kind.

Publishing is after all a nasty business full of pirates selling their dubious wares and posers of all stripes.

Reminds me of this HST quote. He could very well have been speaking of the book publishing or Corporate Internet monopolies.

"The music business is a cruel and shallow money trench, a long plastic hallway where thieves and pimps run free, and good men die like dogs. There's also a negative side."
Hunter S. Thompson

"Publishing is a long game, keep writing and persevering. I wish you nothing but the greatest success."

"Because we're a small press with limited resources, we could not possibly produce such a finely printed and in-color version of the book sent to us. Nonetheless, it's a very ambitious project, and the baseball portions offered appeal."

The hardest part of writing a book is not putting the words on paper, but placing it with the right publisher. We do wish you the very best of luck in finding one who is right.

And then there were the unanticipated reactions:

Hello Writer,
Thank you for submitting your manuscript to Acme Publishing and for your patience as we reviewed your story, which we read with great interest. Although we all liked the concept of your story, unfortunately, we cannot make an offer of publication at this time. Your writing style is impressive, and this is certainly a unique piece. That said, Acme Publishing may not be the best fit in terms of content. We do not have sufficient technical knowledge to assist with this project. Additionally, another publishing company may be able to market your book better.

Dear Writer,
Thank you for your patience in hearing from us about your book. I have unfortunately decided to step aside on representation. My primary reason relates to your platform. Publishers expect authors to have well-developed platforms prior to seeking publication so that they have a built in audience when the book comes out. If a publisher does not believe that the author can sell many thousands of copies on their own, they are averse to taking a project on. This is particularly true of the major NY publishers, whom we pitch to. While I can tell you are doing good work in developing your platform, it still feels a bit early to me to approach NY publishers. I sense that Acme Literary Agency would struggle to find your book a home and for that reason.

Below is a sample query for this book as being a part of a larger trilogy, which was sent, undeterred, to the hundred or so prior queries that had received a response or a rejection. This response or rejection was frequently from a person other than to whom the original query was addressed.

Mr. Joe Blow
Editor
Acme Publishing LTD
Dear Mr. Blow,
I am pitching you a three-volume set of novels. The final volume is nearing completion now. This collection represents my lifetime opus in the form of a bildungsroman extravaganza representing more than ten years of work and fifty years of research and life experience.
These books, as well as this query, will break most book publishing rules by not being traditional, or even suitable for standard print publishing due to cost and complexity. They are also not suitable for Kindle book sausage grinder digital conversion for reasons of quality, style, and complexity, and just as a general principle. PDF files will be the only ascetically and functionally acceptable digital distribution model. These books are:

Book One

- *The Insider (A Life Inside the Personal Computer)*

Approximately 98k words, 350 pages complete
Approximately 125 footnotes, 150 illustrations

Book Two

- *The Cozening (A Murder of Promise)*

Approximately 80k words, 300 pages complete
Approximately 100 footnotes, 200 illustrations.

Book Three

- *The Insider Goes Deep (Tales from the Dark Web)*

Approximately 100k words, 400 pages TBD
Approximately 50 footnotes, 200 illustrations
Approximately 200 CW links and 50 DW links
Approximately 30 Notes

This Insider Goes Deep title is a sequel to the writers' previous two books and follows the continued corruption of computer operating systems and software programs to support the devolution of the original Internet into an individualized predatory surveillance system, corporate ATM, and a global societal menace whose parasitic effects, and predatory behavior threaten lives, freedom, and democracy.

There is now a fourth book as an outgrowth of the extensive research done for the third book, which I see as a companion book:

Book Four
A User Guide To The Dark Web
(The 42nd and Final Encyclopedia Cyberspacia)
Approximately 70k words, 500 pages TBD
Approximately 30 footnotes, 300 illustrations
Approximately 400 CW links and 200 DW links
Approximately 40 Notes

As both a person and as a writer, I have no and have never had any social media presence for both personal and professional reasons which are clearly detailed in the content of these books. Nor do I intend to have any, as this is not relevant to my target demographic.
I have embedded an edgy Prologue excerpt from the third book below for your consideration. I can also forward TOC's or additional content, for each book if you are further interested.

Thank you for your time,

Sincerely,
Prospective Author

Questions for the author

Write to the author at lefty at tcw dot org on the unencrypted clear Internet email systems or via encrypted Tor email at

n0stis@mail2tor.com

What led you to seek out and explore the Dark Web?

For research to write a book, and to follow my curiosity. No really, I wanted to examine the section of cyberspace the way you would if you were considering a new place to work and live if you were to move to a new city.

Weren't you afraid of being busted?

Not really. Did not plan to do anything illegal. If viewing this part of the Internet was a crime, I needed to find this out for myself. And I really did not believe that it was. At least not yet.

What software tools did you use?

A VPN and Tor as outlined in the book.

What did you find there?

Less than I expected. Mostly commerce i.e. buying and selling and things related to the crypto currencies required for transactions.

Who lives there?

Serious computer geeks/math heads, libertarians, malcontents (like me), criminals, drug users, annoying people, etc.

Why not just use the regular web?

As corporate America assimilates and degrades the Internet for their profit purposes, it is becoming less and less usable for regular folks who have an interest in their privacy and wellbeing.

What computer OS do you use?

Lefty aka, n0sits is a strong supporter of the best OS ever written, Windows 7 Ultimate 64-bit. He also supports MS releasing it rights and making this software Freeware.

https://www.fsf.org/windows/upcycle-windows-7

Do you have a website?

Not on the Dark Web, but on the Clear Web. See example below.

https://www.tcw.org/

My books are also for sale here.

Where do you go from here?

As in most of my life, I will bypass the straight line and seek a more interesting detour.

I will continue to work telling stories in my technology cave.

The Insider Writer website

In a Time of Universal Deceit — Telling the Truth Is a Revolutionary Act, and this kind of Courage becomes Contagious

This is where you will find my essays, short stories, and novels.

"We cannot solve our problems with the same thinking we used when we created them." Albert Einstein

Readers beware; these essays may interest, inform, enlighten, enrich, amuse you, dispel myths, theories, and speculation, annoy, agitate, anger, infuriate, and even aggravate you with reality.

It seems to me that we are at a time where we are lacking civil reason and factual debate in this county. Our two party political system is supposed to, and previously did, provide for some measure of the exchange of ideas and compromises based in good faith and on a common understanding of verifiable facts. Now we cannot even agree on facts, although just like the study of the sciences, they are a bit stubborn in that facts are not dependent on whether or not you believe them. We seem to be information rich, yet knowledge and wisdom poor. Foresight flows from the latter two, and not the first.

These essays represent knowledge, insights, and expertise gained from experience and based on factual information. The wisdom and foresight parts are up to the reader. You can think of these essays as crib notes for your busy lives. More than anything, I strive to be factual, accurate, sincere, and honest using the scientific method of linking the original source material directly to the essay.

If you take the blue pill, and create and live in your own reality, you will be constantly challenged and confronted by the actuality of and conflicts with the real world around you. These continuous conflicts may lead you to magical thinking, a belief in the false constructs of the supernatural, the coming of a rapture, and the hope of a better afterlife. But this world will ultimately leave you feeling a hopelessness and depression resulting for many in alcoholism, drug addiction, and suicide. The human mind is like a boomerang in that if you throw it too far, it may not come back.

If however you take the red pill as I suggest you do, you will need to actively deal with the complex, dirty, and often confusing and disgusting world around you. This will eventually lead you to the obvious conclusion that you need to become engaged to try to make the world around you a better place in any way you can. This is of course a responsibility you have as a human being, because if you are not here to make the world a better place, then why are you here? To use a metaphor, you cannot feed all the birds during the winter, but you can feed the ones in your backyard. And so can your neighbor and their neighbors and so on.

I know, I know, there is too much out there for you to care about these days. You are being bombarded with information, misinformation, and disinformation. As a result, you now have too many browser tabs open, so to speak. You are being subjected to the theft and misuse of your personal information by dystopian surveillance machines disguised as your personal devices. Your memory is almost full, and your brain computer feels like it is about to crash with a BSoD (Blue Screen of Death). Beyond your currently open tabs for taking care of yourself and your family, in these essays I will give you a few important tabs I think you should keep open...at least for a while.

Did you listen to music when you wrote this book, and if so what music?

Mostly it was Tom Petty and Jackson Browne on YouTube that made up the sound track for my third book.

I burned through and wore out most everything else I have in my record library on the first two books. ☺

Music Play List

If you hyphenate these site links as yout-ube.com it will take you to https://www.youtube-nocookie.com/ (playlist file) expand the screen and play entirely without commercials.

https://www.youtube.com/watch?v=ascEnKGjph4

Tom Petty and the Heartbreakers Live USA 2003
(Melinda and Shadow People are such a great songs)

https://www.youtube.com/watch?v=5X6IkI_ieSE

(Petty Live at Fenway Park)

https://www.youtube.com/watch?v=yLl2_JIlKps

Tom Petty and the Heartbreakers - Live at the Olympic: The Last DJ (2002) (This one with a full orchestra)

https://www.youtube.com/watch?v=tRdVIsq11-E

Tom Petty And The Heartbreakers - (Wells Fargo Center) Philadelphia, PA 9.15.14 (HD Multicam)

https://www.youtube.com/watch?v=wwLDiDU3KVc

Tom Petty and the Heartbreakers - Live in Chicago, Illinois (1995)

https://www.youtube.com/watch?v=fWfb44z8-RQ

Tom Petty and the Heartbreakers - Live In Dortmund (1982)

https://www.youtube.com/watch?v=1fgZ0xnDgSw

Live at the Bonnaroo Music Festival

https://www.youtube.com/watch?v=3gvA9XrAwzs

Tom Petty and the Heartbreakers - Lockn' Festival (Audio only) (2014)

https://www.youtube.com/watch?v=xk3808yTSKg

Tom Petty and the Heartbreakers live at Piazza Napoleone in Lucca, Italy on June 29th 2012

https://www.youtube.com/watch?v=d5lOIYLQZtY

Tom Petty and the Heartbreakers - Live at the Vic Theatre (2003)

https://www.youtube.com/watch?v=pg_AZajJRlU

Tom Petty and the Heartbreakers - Live In Tuscaloosa, Alabama (1995)

https://www.youtube.com/watch?v=-m__8uMYbkw

Tom Petty And The Heartbreakers - (PPL Center) Allentown, PA 9.16.14 (Complete Show)

https://www.youtube.com/watch?v=pn1Fa-sPA-E

Tom Petty & the HBs Live at Jones Beach 2005-06-21

https://www.youtube.com/watch?v=iBPjKLP7T1o&list=-PL7C13F1EF2BC23072

Tom Petty - The Live Anthology (4 CD)

https://www.youtube.com/watch?v=F6s_-QLGwLk

Tom Petty & the HBs Live at Madison Square Garden 2006-06-20 with Stevie Nicks

https://www.youtube.com/watch?v=4f2UdhTiYlg

Tom Petty and the Heartbreakers Toronto 3/17/95 Full Concert

https://www.youtube.com/watch?v=WblnLk387u0

Tom Petty: Somewhere You Feel Free - The Making of Wildflowers

https://www.youtube.com/watch?v=xKl8tSQFlJg

Tom Petty & The Heartbreakers 1978 06 08 BBC Television - Old Grey Whistle Test

https://www.youtube.com/watch?v=d0qBZuBboVE

Tom Petty 2017 05 05 West Palm Beach, Florida - Perfect Vodka Amphitheater

https://www.youtube.com/watch?v=LwX8dRS4DoY

Tom Petty - Wildflowers (Full Album)

https://www.youtube.com/watch?v=82jXfi5fW8c

Tom Petty (Vinyl) Damn the Torpedoes (full album)

https://www.youtube.com/watch?v=xBscCC-cyfE

Tom Petty - New York 1999 JEMS Soundboard

https://www.youtube.com/watch?v=Vjx_ynNHweg

Tom Petty and the Heartbreakers 1994.10.02 Bridge School Mountain View, CA

https://www.youtube.com/watch?v=pXStJ0rOokU

Tom Petty - Bridge School Benefit (1986)

https://www.youtube.com/watch?v=TycUk59Rm7A

Tom Petty and the Heartbreakers - Rock Goes To College (1980)

https://www.youtube.com/watch?v=IaHxPi9dM7o

JJ Cale & Leon Russell at the Paradise Studios, LA 1979

https://www.youtube.com/watch?v=Ai7TjHuZ8Uk

Jackson Browne - I'll Do Anything: Live In Concert

https://www.youtube.com/watch?v=SmlRXhjulHg

Jackson Browne Greatest Hits || Jackson Browne Playlist

https://www.youtube.com/watch?v=4UyrPxLUYJI

Jackson Browne Greatest Hits Full Album || Jackson Browne Best Songs Non-Stop Playlist

https://www.youtube.com/watch?v=rwvZMepkOOc

Traveling Wilburys – Volume 1 (Full Album)

https://www.youtube.com/watch?v=d7PsHS_vixU

The Very Best of Steely Dan

https://www.youtube-nocookie.com/embed/RxJLss9DdUs?playlist=RxJLss-9DdUs&autoplay=1&iv_load_policy=3&loop=-1&modestbranding=1&start

Best Songs Of Pink Floyd | Pink Floyd Greatest Hits of All Time

https://www.youtube.com/watch?v=mMTVXDu5v5U

David Gilmour in Concert The Meltdown Concert 2002 (Comfortably Numb at 43.50 to 50:30) Oh My!

https://www.youtube-nocookie.com/embed/E9Iau_oik-E?playlist=E9Iau_oik-E&autoplay=1&iv_load_policy=3&loop=1&modestbranding=1&start=

Pink Floyd-Pulse Live 1994 Remastered

https://www.youtube-nocookie.com/embed/ff7Fo8LHhPk?playlist=ff7Fo8LHhPk&autoplay=1&iv_load_policy=3&loop=1&modestbranding=1&start=

Paul McCartney Unplugged Mtv 1991 HD

https://www.youtube.com/watch?v=9elQeVfrLOo

Paul McCartney: Chaos and Creation At Abbey Road
Some of this is tedious, but hang with it as it is great. Big finish!

https://www.youtube-nocookie.com/embed/wmx-nxjuVq4?playlist=wmx-nxjuVq4&autoplay=1&iv_load_policy=3&loop=1&modestbranding=1&start=

Paul McCartney on NPR with Terry Gross (November 3, 2021)

If you like Springsteen you should love this next one.

https://youtu.be/s79tVdT2jUs?list=TLGGzo7kzd99GZ-4yMDA0MjAyMg

Lost In the Flood (Live at the Hammersmith Odeon, London '75)

https://www.youtube-nocookie.com/embed/3blzcipjK3s?playlist=-3blzcipjK3s&autoplay=1&iv_load_policy=3&loop=-1&modestbranding=1&start=

Madison Square Garden January 27 2016 Bruce Springsteen and the E Street Band (The camera work is bad, so just listen to some perfection)

https://www.youtube.com/watch?v=BhbhiQZwjf4

Productive Music Radio — Future Garage for Smooth Workflow

https://www.youtube.com/watch?v=FuaQ1QhJOkc&list=PLdE7uo_-7KBkfAWkk7-Clm18krBuziKQfr&index=4

Deep Programming Music — Coding Skills — Night Work Chillstep

https://www.youtube.com/watch?v=apkw9zKcAg0&list=PLgHsCMaUelhkLf83d3JdVZtuzatGgSpdD&index=2

24 songs from one of the greatest singers and songwriters of our time, Jackson Browne

https://www.youtube.com/watch?v=Ai7TjHuZ8Uk

Jackson Browne - I'll Do Anything: Live In Concert

The Heroes of our Time

Whistleblower Hall of Fame

Julian Assange

Julian Paul Assange né Hawkins; born 3 July 1971 is an Australian editor, publisher and activist who founded WikiLeaks in 2006. WikiLeaks came to international attention in 2010 when it published a series of leaks provided by U.S. Army intelligence analyst Chelsea Manning. These leaks included the Baghdad airstrike Collateral Murder video (April 2010), the Afghanistan war logs (July 2010), the Iraq war logs (October 2010), and Cablegate (November 2010). After the 2010 leaks, the United States government launched a criminal investigation into WikiLeaks.

In November 2010, Sweden issued an international arrest warrant for Assange over allegations of sexual misconduct. Assange said the allegations were a pretext for his extradition from Sweden to the United States over his role in the publication of secret American documents. After losing his battle against extradition to Sweden, he breached bail and took refuge in the Embassy of Ecuador in London in June 2012. He was granted asylum by Ecuador in August 2012 on the grounds of political persecution, with the presumption that if he were extradited to Sweden, he would be eventually extradited to the United States. Swedish prosecutors dropped their investigation in 2019, saying their evidence had "weakened considerably due to the long period of time that has elapsed since the events in question".

During the 2016 U.S. election campaign, WikiLeaks published confidential Democratic Party emails, showing that the party's national committee favored Hillary Clinton over her rival Bernie Sanders in the primaries.

On 11 April 2019, Assange's asylum was withdrawn following a series of disputes with the Ecuadorian authorities. The police were invited into the embassy and he was arrested.[16] He was found guilty of breaching the Bail Act and sentenced to 50 weeks in prison. The United States government unsealed an indictment against Assange related to the leaks provided by Manning. On 23 May 2019, the United States government further charged Assange with violating the Espionage Act of 1917. Editors from newspapers, including The Washington Post and The New York Times, as well as press freedom organisations, criticized the government's decision to charge Assange under the Espionage Act, characterizing it as an attack on the First Amendment to the United States Constitution, which guarantees freedom of the press.

On 4 January 2021, UK District Judge Vanessa Baraitser ruled against the United States' request to extradite Assange and stated that doing so would be "oppressive" given concerns over Assange's mental health and risk of suicide. On 6 January 2021, Assange was denied bail, pending an appeal by the United States. On 10 December 2021, the High Court in London ruled that Assange could be extradited to the US to face the charges. In March 2022, the UK Supreme Court refused Assange permission to appeal.

Assange has been confined in Belmarsh maximum-security prison in London since April 2019.

https://en.wikipedia.org/wiki/Julian_Assange

He has done no more than tell the world about criminal military planning and policies, and the horrors of wars in Afghanistan and Iraq. He deserves to be thanked.

Ed Snowden

Edward Joseph Snowden (born June 21, 1983) is an American former computer intelligence consultant who leaked highly classified information from the National Security Agency (NSA) in 2013, when he was an employee and subcontractor. His disclosures revealed numerous global surveillance programs, many run by the NSA and the Five Eyes Intelligence Alliance with the cooperation of telecommunication companies and European governments, and prompted a cultural discussion about national security and individual privacy.

In 2013, Snowden was hired by an NSA contractor, Booz Allen Hamilton, after previous employment with Dell and the CIA. Snowden says he gradually became disillusioned with the programs with which he was involved, and that he tried to raise his ethical concerns through internal channels but was ignored. On May 20, 2013, Snowden flew to Hong Kong after leaving his job at an NSA facility in Hawaii, and in early June he revealed thousands of classified NSA documents to journalists Glenn Greenwald, Laura Poitras, Barton Gellman, and Ewen MacAskill. Snowden came to international attention after stories based on the material appeared in The Guardian, The Washington Post, and other publications. Snowden also made extensive allegations against the GCSB, blowing the whistle of their domestic surveillance of New Zealanders and acts of espionage under John Key's government.

On June 21, 2013, the United States Department of Justice unsealed charges against Snowden of two counts of violating the Espionage Act of 1917 and theft of government property, following which the Department of State revoked his passport. Two days later, he flew into Moscow's Sheremetyevo International Airport, where Russian authorities observed the canceled passport, and he was restricted to the airport terminal for over one month. Russia later granted Snowden the right of asylum with an initial visa for residence for one year, which was subsequently repeatedly extended. In October 2020, he was granted permanent residency in Russia.

A subject of controversy, Snowden has been variously called a traitor, a hero a whistleblower, a dissident, a coward, and a patriot. U.S. officials condemned his actions as having done "grave damage" to the U.S. intelligence capabilities. Snowden has defended his leaks as an effort "to inform the public as to that which is done in their name and that which is done against them." His disclosures have fueled debates over mass surveillance, government secrecy, and the balance between national security and information privacy, something that he has said he intended to do in retrospective interviews.

In early 2016, Snowden became the president of the Freedom of the Press Foundation, a San Francisco–based nonprofit organization that aims to protect journalists from hacking and government surveillance. He also has a job at an unnamed Russian IT company. In 2017, he married Lindsay Mills. On September 17, 2019, his memoir Permanent Record was published. On September 2, 2020, a U.S. federal court ruled in United States v. Moalin that the U.S. intelligence's mass surveillance program exposed by Snowden was illegal and possibly unconstitutional.

https://en.wikipedia.org/wiki/Edward_Snowden

Chelsea Manning

Chelsea Elizabeth Manning (born Bradley Edward Manning, December 17, 1987) is an American activist and whistleblower. She is a former United States Army soldier who was convicted by court-martial in July 2013 of violations of the Espionage Act and other offenses, after disclosing to WikiLeaks nearly 750,000 classified, or unclassified but sensitive, military and diplomatic documents. She was imprisoned from 2010 until 2017 when her sentence was commuted. A trans woman, Manning stated in 2013 that she had a female gender identity since childhood and wanted to be known as Chelsea Manning. She also expressed a desire to begin hormone replacement therapy.

Assigned in 2009 to an Army unit in Iraq as an intelligence analyst, Manning had access to classified databases. In early 2010, she leaked classified information to WikiLeaks and confided this to Adrian Lamo, an online acquaintance.[10] Lamo indirectly informed the Army's Criminal Investigation Command, and Manning was arrested in May that same year. The material included videos of the July 12, 2007, Baghdad airstrike and the 2009 Granai airstrike in Afghanistan; 251,287 U.S. diplomatic cables; and 482,832 Army reports that came to be known as the "Iraq War Logs" and "Afghan War Diary". The material was published by WikiLeaks and its media partners between April 2010 and April 2011.

Manning was charged with 22 offenses, including aiding the enemy, which was the most serious charge and could have resulted in a death sentence. She was held at the Marine Corps Brig, Quantico in Virginia, from July 2010 to April 2011, under Prevention of Injury status—which entailed de facto solitary confinement and other restrictions that caused domestic and international concern—before being transferred to the Joint Regional Correctional Facility at Fort Leavenworth, Kansas, where she could interact with other detainees. She pleaded guilty in February 2013 to 10 of the charges. The trial on the remaining charges began on June 3, 2013, and on July 30, she was convicted of 17 of the original charges and

amended versions of four others, but was acquitted of aiding the enemy. She was sentenced to 35 years at the maximum-security U.S. Disciplinary Barracks at Fort Leavenworth. On January 17, 2017, President Barack Obama commuted Manning's sentence to nearly seven years of confinement dating from her arrest on May 27, 2010. After release, Manning earned a living through speaking engagements.

In 2018, Manning challenged incumbent Senator Ben Cardin for the Democratic nomination for the United States Senate election in her home state of Maryland.[24] Manning received 5.8% of the votes; Cardin won re-nomination with 80.4% of the votes cast. From March 8, 2019, to March 12, 2020 (except for a week from May 9 to 16), Manning was jailed for contempt and fined $256,000 for refusing to testify before a grand jury investigating WikiLeaks founder Julian Assange.

Reality Winner

Reality Leigh Winner is a former American intelligence specialist, charged with "removing classified material from a government facility and mailing it to a news outlet." The subject material originated from the National Security Agency (NSA). On June 3, 2017, while employed by military contractor Pluribus International Corporation, Winner was arrested on suspicion of leaking an intelligence report about Russian interference in the 2016 United States elections to the news website The Intercept. The report suggested that Russian hackers attacked a U.S. voting software supplier. Denied bond, Winner is being held at the Lincoln County Jail in Lincolnton, Georgia.

Winner was charged with "removing classified material from a government facility and mailing it to a news outlet." On June 8, 2017, she pleaded not guilty to a charge of "willful retention and transmission of national defense information," and was denied bail. Prosecutors alleged she may have been involved in other leaks of classified information, and might try to flee the country if released. Justice Department lawyers also

argued that her defense team should not be allowed to discuss any classified information, even if it was in news reports published by the media.

On August 29, 2017, Winner's attorneys filed a motion in district court to suppress her statements to law enforcement, arguing that Winner was not read her Miranda rights before being interrogated by the FBI on June 3. On October 5, 2017, Judge Brian Epps denied a second request from her defense attorneys that bail be set. In December 2017, The Intercept reported that Winner's defense team was allowed to discuss the case with her, including its classified aspects, in a Sensitive Compartmented Information Facility (SCIF).[50] First Look, the parent company of The Intercept, helped fund her defense, and as of September 2020 was still paying her legal bills.

On January 31, 2018, the U.S. Court of Appeals for the Eleventh Circuit affirmed a lower court order blocking Winner from posting bond, determining that no combination of conditions would reasonably assure her presence at trial, thus ensuring that she remained in jail until her trial, which was scheduled to begin on October 15, 2018.

A "Stand with Reality" campaign was formed by representatives from Courage to Resist, the Electronic Frontier Foundation and the Freedom of the Press Foundation with the goal of "raising public awareness" to ensure that Reality Winner received a fair trial.[55] Billie Winner-Davis, mother of Reality Winner, called on members of the public to join the campaign.

On June 21, 2018, Winner asked the court to allow her to change her plea to guilty. On June 26, she pleaded guilty to one count of felony transmission of national defense information. Winner's plea agreement with prosecutors called for her to serve five years and three months in prison followed by three years of supervised release.

On August 23, 2018, Winner was sentenced to the agreed-upon five years and three months in prison for violating the Espionage Act of 1917. Prosecutors said her sentence, sixty-three months in prison, was the longest ever imposed in federal court for an unauthorized release of government information to the media. The New York Times reported, "Under the plea agreement, Ms. Winner will be transferred to the Federal Bureau of Prisons Federal Medical Center, Carswell in Fort Worth, Texas, where she can receive treatment for bulimia and be relatively close to her family."

On August 24, President Donald Trump tweeted, "Ex-NSA contractor to spend 63 months in jail over 'classified' information. Gee, this is 'small potatoes' compared to what Hillary Clinton did! So unfair Jeff, Double Standard." Winner expressed ironic appreciation for Trump's support, saying, "I can't thank him enough." Titus Nichols, Winner's lawyer, called the tweet "bizarre" and that it was just Trump "taking aim at Sessions". On August 31, Winner said that she would ask Trump for clemency as a result of his tweet, adding that her legal team was already working on her pardon application.

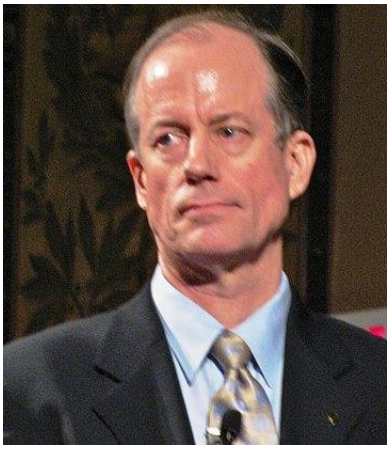
In 2019, The Guardian compared Winner's case to those of Daniel Everett Hale and of Henry Kyle Frese.

On April 24, 2020, a federal judge rejected Winner's request to commute the remaining 19 months of her 63-month sentence and be released to home confinement due to the COVID-19 pandemic. Winner's lawyer argued that her history of respiratory illness and immune system compromised by bulimia makes her highly vulnerable to the virus. Two inmates had tested positive before Winner was transferred to the center where, under the terms of her June 2018 guilty plea agreement, Winner was housed to meet her special needs. She was immediately quarantined and never entered the general population there. The government insisted that the Bureau of Prisons "has taken aggressive action to mitigate the danger and is taking careful steps to protect inmates' and BOP staff members' health." The judge found that Winner did not exhaust her administrative remedies through the BOP, which he held has sole authority to grant her compassionate release.

Winner tested positive for COVID-19 in July 2020. By September 13, 2020, Winner was recovering from the coronavirus, although still experiencing occasional shortness of breath.

On June 2, 2021, Winner was transferred from prison to a transitional facility, the San Antonio, Texas, Residential Reentry Management center. According to Alison Grinter Allen, Winner's lawyer, she left prison early as a result of "good behavior" while inside, and not because of compassionate release. Betsy Reed, the editor-in-chief of The Intercept, commented, "Selective and politically motivated prosecutions of leakers and whistleblowers under the Espionage Act – which dramatically escalated under Barack Obama, opening the door for the Trump justice department's abuses – are an attack on the First Amendment that will one day be judged harshly by history."

https://en.wikipedia.org/wiki/Reality_Winner



Thomas Drake

Thomas Andrews Drake (born 1957) is a former senior executive of the National Security Agency (NSA), a decorated United States Air Force and United States Navy veteran, and a whistleblower. In 2010, the government alleged that Drake mishandled documents, one of the few such Espionage Act cases in U.S. history. Drake's defenders claim that he was instead being persecuted for challenging the Trailblazer Project. He is the 2011 recipient of the Ridenhour Prize for Truth-Telling and co-recipient of the Sam Adams Associates for Integrity in Intelligence (SAAII) award.

On June 9, 2011, all 10 original charges against him were dropped. Drake rejected several deals because he refused to "plea bargain with the truth". He eventually pleaded to one misdemeanor count for exceeding authorized use of a computer; Jesselyn Radack of the Government Accountability Project, who helped represent him, called it an act of civil disobedience.

https://en.wikipedia.org/wiki/Thomas_A._Drake

Bill Binney

William Edward Binney is a former intelligence official with the United States National Security Agency (NSA) and whistleblower. He retired on October 31, 2001, after more than 30 years with the agency.

In September 2002, he, along with J. Kirk Wiebe and Edward Loomis, asked the U.S. Defense Department Inspector General (DoD IG) to investigate the NSA for allegedly wasting "millions and millions of dollars" on Trailblazer, a system intended to analyze mass collection of data carried on communications networks such as the Internet. Binney had been one of the inventors of an alternative system, ThinThread, which was shelved when Trailblazer was chosen instead. Binney has also been publicly critical of the NSA for spying on U.S. citizens, saying of its expanded surveillance after the September 11, 2001 attacks that "it's better than anything that the KGB, the Stasi, or the Gestapo and SS ever had" as well as noting Trailblazer's ineffectiveness and unjustified high cost compared to the far less intrusive ThinThread. He was furious that the NSA hadn't uncovered the 9/11 plot and stated that intercepts it had collected but not analyzed likely would have garnered timely attention with his leaner more focused system.

He later criticized the NSA's data-collection policies during the Barack Obama administration.

https://en.wikipedia.org/wiki/William_Binney_-(intelligence_official)

Aaron Schwartz

Aaron Hillel Swartz (November 8, 1986 – January 11, 2013) was an American computer programmer, entrepreneur, writer, political organizer, and Internet hacktivist. He was involved in the development of the web feed format RSS, the Markdown publishing format, the organization Creative Commons, the website framework web.py, and joined the social news site Reddit six months after its founding. He was given the title of co-founder of Reddit by Y Combinator owner Paul Graham after the formation of Not a Bug, Inc. (a merger of Swartz's project Infogami and Redbrick Solutions, a company run by Alexis Ohanian and Steve Huffman). Swartz's work also focused on civic awareness and activism. He helped launch the Progressive Change Campaign Committee in 2009 to learn more about effective online activism. In 2010, he became a research fellow at Harvard University's Safra Research Lab on Institutional Corruption, directed by Lawrence Lessig. He founded the online group Demand Progress, known for its campaign against the Stop Online Piracy Act.

In 2011, Swartz was arrested by Massachusetts Institute of Technology (MIT) police on state breaking-and-entering charges, after connecting a computer to the MIT network in an unmarked and unlocked closet, and setting it to download academic journal articles systematically from JSTOR using a guest user account issued to him by MIT. Federal prosecutors, led by Carmen Ortiz, later charged him with two counts of wire fraud and eleven violations of the Computer Fraud and Abuse Act, carrying a cumulative maximum penalty of $1 million in fines, 35 years in prison, asset forfeiture, restitution, and supervised release. Swartz declined a plea bargain under which he would have served six months in federal prison. Two days after the prosecution rejected a counter-offer by Swartz, he was found dead by suicide in his Brooklyn apartment. In 2013, Swartz was inducted posthumously into the Internet Hall of Fame.

https://en.wikipedia.org/wiki/Aaron_Swartz

Daniel Hale

Daniel Everette Hale (born 1987/1988) is a former National Security Agency (NSA) intelligence analyst who leaked classified information about drone warfare to the press.

Hale served in the United States Air Force 2009-2013 before joining the National Security Agency and leaking classified documents to The Intercept.

Hale served in the United States Air Force from July 2009 to July 2013. He was an enlisted airman. In 2013, he was assigned to the NSA and the Joint Special Operations Command at Bagram Airfield, the largest U.S. military base in Afghanistan, where he helped identify targets for assassination. In February 2014, after leaving the Air Force and becoming a contractor at the National Geospatial-Intelligence Agency, Hale leaked 17 classified documents to The Intercept. The documents contained details about U.S. kill lists and civilian casualties of drone strikes, and in some cases revealed actions that, if proven, would amount to war crimes. The documents formed the basis of a series of articles, the "Drone Papers", published by The Intercept in October 2015.

Marjorie Cohn writing for Truthout reported that, 'During one five-month period during January 2012 to February 2013, nearly 90 percent of those killed by drone strikes were not the intended target ... . But civilian bystanders were nonetheless classified as “enemies killed in action” unless proven otherwise.

On August 8th, 2014, the FBI raided his home in Lorton, Virginia, in what he described as retribution for his political activism. In 2016, he appeared in the documentary film National Bird, where he described his crisis of conscience and the FBI raid.

In 2019, Hale was charged with disclosing intelligence information and theft of government property. He was arraigned in the U.S. District Court for the Eastern District of Virginia. In March 2021, he pleaded guilty to retaining and transmitting national defense information. On July 27, 2021, citing the need to deter others from disclosing government secrets, U.S. District Judge Liam O'Grady sentenced Hale to 45 months in prison for violating the Espionage Act of 1917. "You are not being prosecuted for

speaking out about the drone program killing innocent people", O'Grady told Hale. "You could have been a whistleblower ... without taking any of these documents. “In court, Hale said he accepted punishment for taking the documents, and for taking innocent lives during his participation in the drone program. Noting that he is a descendant of Nathan Hale, executed for spying on the British for the Continental Army during the American Revolutionary War, Hale paraphrased his ancestor's reported last words, saying, "I have but this one life to give in service of my country."

Following sentencing, Hale was transferred from Alexandria City Jail to temporary confinement at Northern Neck Regional Jail in Virginia to await further disposition. In early October 2021, Hale was transferred to a Communications management unit in the United States Penitentiary, Marion, Illinois.

In August 2021 he received the Sam Adams Award for Integrity in Intelligence, eponymously named for a Vietnam War-era whistleblower, for "performing a vital public service at great personal cost—imprisonment for truth-telling". Later that month, U.S. Representative Ilhan Omar (D-MN) wrote to President Biden requesting a full pardon or commutation of sentence for Hale.

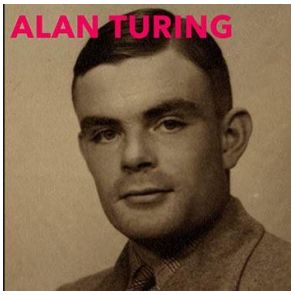
https://en.wikipedia.org/wiki/Daniel_Hale

Jeffrey Alexander Sterling is an American lawyer and former CIA employee who was arrested, charged, and convicted of violating the Espionage Act for revealing details about Operation Merlin (covert operation to supply Iran with flawed nuclear warhead blueprints) to journalist James Risen. The case was based on what the judge called "very powerful circumstantial evidence." In May 2015, Sterling was sentenced to 3½ years in prison. In 2016 and 2017, he filed complaints and wrote letters regarding mistreatment, lack of medical treatment for life-threatening conditions, and false allegations against him by corrections officers leading to further punitive measures. He was released from prison in January 2018.

https://en.wikipedia.org/wiki/Jeffrey_Alexander_Sterling

There is always room for more heroes. How about you?

Hero's Hall of Fame



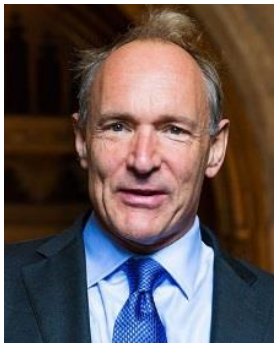
Alan Turing

Alan Mathison Turing (23 June 1912 – 7 June 1954) was an English computer scientist. Turing was highly influential in the providing a formalization of the concepts of algorithm and computation with the Turing machine, a model of a general-purpose computer.

Turing worked for the Government Code and Cypher School at Bletchley Park. He led the section that was responsible for German naval cryptanalysis. Turing played a crucial role in cracking intercepted coded messages that enabled the Allies to defeat the Axis powers.

Turing was prosecuted in 1952 for homosexual acts. He accepted chemical castration, as an alternative to prison. Turing died on 7 June 1954, from cyanide poisoning. A possible suicide, but the known evidence is also consistent with accidental poisoning.

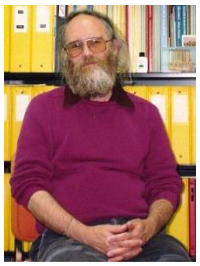
https://en.wikipedia.org/wiki/Alan_Turing



Sir Tim Berners Lee

Created the original Internet Web. On the 25th anniversary of the web Sir Tim Berners Lee when questioned Edward Snowden, Hero or villain? Replied, "The whistleblower may be all that saves our society."

https://en.wikipedia.org/wiki/Tim_Berners-Lee



Jon Postel

Jon Postel one of the fathers of the internet, published RFC 821 on 1 August 1982 a technical paper laying out a standard called Simple Mail Transfer Protocol, or SMTP.

https://en.wikipedia.org/wiki/Jon_Postel

Ladar Levison

He created a, email service called Lavabit, but he closed it in 2014 when FBI agents demanded he silently give up information about one particular Lavabit user: Edward Snowden. Levison refused to give up the encryption keys that would let the feds secretly monitor Lavabit, choosing instead to shut it down.

https://en.wikipedia.org/wiki/Lavabit#Ladar_Levison

Robert William (Bob) Taylor

Robert William Taylor (February 10, 1932 – April 13, 2017), known as Bob Taylor, was an American Internet pioneer, who led teams that made major contributions to the personal computer, and other related technologies. He was director of ARPA's Information Processing Techniques Office from 1965 through 1969, founder and later manager of Xerox PARC's Computer Science Laboratory from 1970 through 1983.

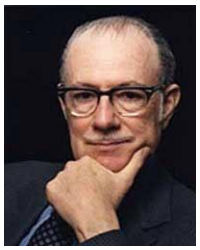
https://en.wikipedia.org/wiki/RobertTaylor

J. C. R. Licklider

Joseph Carl Robnett Licklider March 11, 1915 – June 26, 1990), known simply as J. C. R. or "Lick", was an American psychologist and computer scientist who is considered to be among the most prominent figures in computer science development and general computing history.

He is particularly remembered for being one of the first to foresee modern-style interactive computing and its application to all manner of activities; and also as an Internet pioneer with an early vision of a worldwide computer network long before it was built. He did much to initiate this by funding research which led to much of it, including today's canonical graphical user interface, and the ARPANET, the direct predecessor to the Internet.

https://en.wikipedia.org/wiki/J._C._R._Licklider



George Pake

George E. Pake (April 1, 1924 – March 4, 2004) was a physicist and research executive primarily known for helping founded Xerox PARC. PARC assembled a first-rate collection of research talent, especially in the area of computer science. During Pake's years running Xerox PARC, the research center invented the laser printer and pioneered the use of a computer "desktop" which functioned by clicking on "icons."

https://en.wikipedia.org/wiki/George_Pake

Jerome I. Elkind

Jerome Elkind is an American electrical engineer and computer scientist. In 1988 he was co-founder of the Lexia Institute. Elkind was educated at MIT. He went on to join BBN Technologies and then was appointed head of the Computer Science Laboratory at Xerox's Palo Alto Research Center. He also worked with Bob Taylor on the Xerox Alto.

https://en.wikipedia.org/wiki/Jerome_I._Elkind

David C. Evans

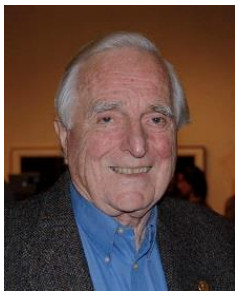
David Cannon Evans (February 24, 1924 – October 3, 1998) was the founder of the computer science department at the University of Utah and co-founder (with Ivan Sutherland) of Evans & Sutherland, a pioneering firm in computer graphics hardware.

https://en.wikipedia.org/wiki/David_C._Evans

Jeff Rulifson

Johns Frederick (Jeff) Rulifson (born August 20, 1941) is an American computer scientist. He led the software team that implemented the oN-Line System (NLS), a system that foreshadowed many future developments in modern computing and networking.

https://en.wikipedia.org/wiki/Jeff_Rulifson



Douglas Engelbart

Douglas Carl Engelbart (January 30, 1925 – July 2, 2013) was an engineer and inventor, and an early computer and Internet pioneer. He is best known for his work on founding the field of human–computer interaction, particularly while at his Augmentation Research Center Lab in SRI International, which resulted in creation of the computer mouse, and the development of hypertext, networked computers, and precursors to graphical user interfaces. These were demonstrated at The Mother of All Demos in 1968. Engelbart's law, the observation that the intrinsic rate of human performance is exponential, is named after him.

https://en.wikipedia.org/wiki/Douglas_Engelbart

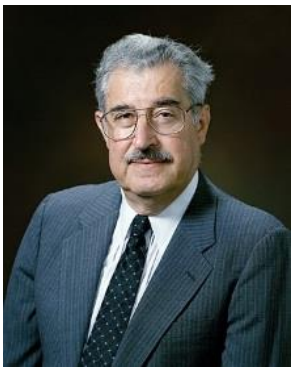
Theodor Nelson

Theodor Holm Nelson (born June 17, 1937) is an American pioneer of information technology, philosopher, and sociologist. He coined the terms hypertext[71], in the 1950s, hypermedia, transclusion, virtuality, and intertwingularity. Nelson founded Project Xanadu in 1960, with the goal of creating a computer network with a simple user interface.

https://en.wikipedia.org/wiki/Ted_Nelson

"Most people are fools, most authority is malignant, God does not exist, and everything is wrong." Ted Nelson

[71] *"Hypertext": Human-readable information linked together in an unconstrained way.*



Charles M. Herzfeld

Charles Maria Herzfeld June 29, 1925 – February 23, 2017 was an Austrian-born American scientist and scientific manager, particularly for the US Government. He is best known for his time as Director of DARPA, during which, among other things, he personally took the decision to authorize the creation of the ARPANET, the predecessor of the Internet.

https://en.wikipedia.org/wiki/Charles_M._Herzfeld

Larry Tesler

Lawrence Gordon Tesler (April 24, 1945 – February 16, 2020) was an American computer scientist who worked in the field of human–computer interaction. Tesler worked at Xerox PARC, Apple, Amazon, and Yahoo! PARC had established development of the Xerox Alto, the first computer system designed around a graphical user interface (GUI). Tesler also was part of a team with Adele Goldberg and Douglas Fairbairn that worked on the Xerox NoteTaker, a portable computer system Alan Kay had envisioned.

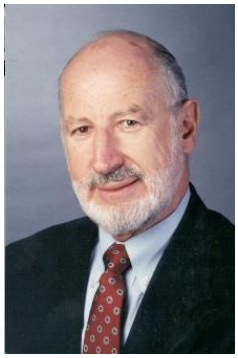
https://en.wikipedia.org/wiki/Larry_Tesler

Alan Kay

Alan Curtis Kay (born May 17, 1940) is an American computer scientist. He is best known for his pioneering work on object-oriented programming and windowing graphical user interface (GUI) design. He received the Turing award in 2003.

While at PARC, Kay conceived the Dynabook concept, a key progenitor of laptop and tablet computers and the e-book. He is also the architect of the modern overlapping windowing graphical user interface (GUI).

https://en.wikipedia.org/wiki/Alan_Kay



Norm Abramson

Norman Abramson is a pioneer in the field of wireless and local area networking. While at the University of Hawaii, he led efforts that gave rise to the construction and operation of the ALOHANet, the first wireless packet network, and to the development of the theory of random access ALOHA channels. ALOHA channels have yielded significant advancements within wireless and local area networking. This influential work also developed the core concepts found today in Ethernet.

https://ethw.org/Norman_Abramson

Judy Estrin

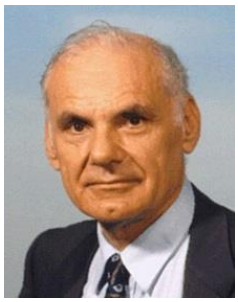
Judith "Judy" L. Estrin (born 1954/1955) is an American entrepreneur, business executive, and philanthropist. Estrin worked with Vinton Cerf on the Transmission Control Protocol project at Stanford University in the 1970s. After Stanford, she worked at a startup semiconductor company called Zilog Corporation that had separated from Intel, where she contributed to the design of the Z8 and Z8000 microprocessors. She led the team that developed one of the first commercial local area network systems called Z-net.

https://en.wikipedia.org/wiki/Judith_Estrin

David Clark

Since the mid-70s, he has been leading the development of the Internet; from 1981-1989 he acted as Chief Protocol Architect in this development, and chaired the Internet Activities Board. His design research looks at re-definition of the architectural underpinnings of the Internet, and the relation of technology and architecture to economic, societal and policy considerations. He supported the U.S. National Science Foundation Future Internet Architecture program.

https://www.csail.mit.edu/person/david-clark



Lawrence G. Roberts

Lawrence Gilman (Larry) Roberts (December 21, 1937 – December 26, 2018) was an American engineer who received the Draper Prize in 2001 "for the development of the Internet".

As a program manager and later office director at the Advanced Research Projects Agency, Roberts and his team created the ARPANET using packet switching techniques invented by British computer scientist Donald Davies and American Paul Baran. The ARPANET, which was built by the Massachusetts-based company Bolt, Beranek, and Newman (BBN), was a predecessor to the modern Internet.

https://en.wikipedia.org/wiki/Lawrence_Roberts_(scientist)

Al Gore

Albert Arnold Gore Jr. (born March 31, 1948) is an American politician and environmentalist and the 45th vice president of the United States from 1993 to 2001 under president Bill Clinton, and a congressman and Senator. Internet pioneers Vint Cerf and Bob Kahn noted that, “as far back as the 1970s, Congressman Gore promoted the idea of high-speed telecommunications as an engine for both economic growth and the improvement of our educational system. He was the first elected official to grasp the potential of computer communications to have a broader impact than just improving the conduct of science and scholarship. When the Internet was still in the early stages of its deployment, Congressman Gore provided intellectual leadership by helping create the vision of the potential benefits of high speed computing and communication.”

https://en.wikipedia.org/wiki/Al_Gore

Dave Crocker

Dave started his networking career In the 1970's, when he worked for four years at UCLA with ARPANET.

He has managed development of the TCP/IP stack at Ungermann-Bass, Inc. and was co-architect and Director of System Development at MCI Digital Information Services Corp, where he worked with Vint Cerf to build a national email service.

Prior to this, he worked as the Co-Principal Investigator, for the CSNet project and an ARPA/Internet email gateway project, housed at the University of Delaware. For his work on email, Dave was a co-recipient of the 2004 IEEE Internet Award.

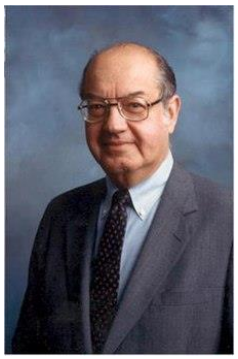
https://icannwiki.org/Dave_Crocker

Vannevar Bush

Vannevar Bush (March 11, 1890 – June 28, 1974) was an American engineer, inventor and science administrator, and was chiefly responsible for the movement that led to the creation of the National Science Foundation. The funding agency of the early Internet.

During his career, Bush patented a string of his own inventions. He is known particularly for his engineering work on analog computers, and for the Memex. The Memex, which he began developing in the 1930s (heavily influenced by Emanuel Goldberg's "Statistical Machine" from 1928) was a hypothetical adjustable microfilm viewer with a structure analogous to that of hypertext. The Memex and Bush's 1945 essay "As We May Think" influenced generations of computer scientists, who drew inspiration from his vision of the future.

https://en.wikipedia.org/wiki/Vannevar_Bush



Paul Baran

Paul Baran (born Pesach Baran (April 29, 1926 – March 26, 2011) was a Polish-American engineer who was a pioneer in the development of computer networks. He was one of the two independent inventors of packet switching, which is today the dominant basis for data communications in computer networks worldwide, and went on to start several companies and develop other technologies that are an essential part of modern digital communication.

https://en.wikipedia.org/wiki/Paul_Baran

Donald W. Davies

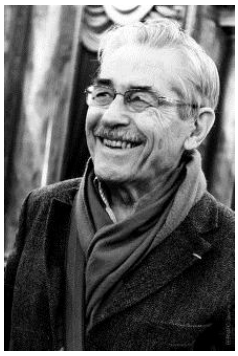
Donald Watts Davies, CBE FRS (7 June 1924 – 28 May 2000) was a Welsh computer scientist who was employed at the UK National Physical Laboratory (NPL). In 1965 he conceived of packet switching, which is today the dominant basis for data communications in computer networks worldwide. Many of the wide-area packet-switched networks built in the 1970s were similar "in nearly all respects" to his original 1965 design. The ARPANET project credited Davies for his influence, which was key to the development of the Internet. Davies' work was independent of the work of Paul Baran in the United States who had a similar idea in the early 1960s, and who also worked on ARPANET.

https://en.wikipedia.org/wiki/Donald_Davies

Leonard Kleinrock

Leonard Kleinrock (born June 13, 1934) is an American computer scientist. A professor at UCLA's Henry Samueli School of Engineering and Applied Science, he made several important contributions to the field of computer science, in particular to the theoretical foundations of data communication in computer networking. He played an influential role in the development of the ARPANET and supervised many graduate students who worked on the communication protocols for internetworking which led to the Internet.

https://en.wikipedia.org/wiki/Leonard_Kleinrock



Louis Pouzin

Louis Pouzin (April 20, 1931 in Chantenay-Saint-Imbert, Nièvre, France) is a French computer scientist. He designed an early packet communications network, CYCLADES.

This network was the first actual implementation of the pure datagram model, initially imagined and described by Donald Davies, subsequently named by Halvor Bothner-By, and seen by Louis Pouzin as his personal invention. His work, and that of his colleagues Hubert Zimmerman and Gérard Le Lann, were acknowledged by Vinton Cerf as substantial contributions to the design of TCP/IP, the protocol suite used by the Internet.

https://en.wikipedia.org/wiki/Louis_Pouzin

Stephen D. Crocker

Stephen D. Crocker (born October 15, 1944) is the inventor of the Request for Comments series, authoring the first RFC and many more. Crocker served as chair of the board of the Internet Corporation for Assigned Names and Numbers, ICANN from 2011 through 2017.

Steve Crocker has worked in the Internet community since its inception. As a UCLA graduate student in the 1960s, he was part of the team that developed the protocols for the ARPANET which were the foundation for today's Internet. For this work, Crocker was awarded the 2002 IEEE Internet Award.

https://en.wikipedia.org/wiki/Steve_Crocker

Grace Hopper

Grace Brewster Murray Hopper (née Murray; December 9, 1906 – January 1, 1992) was an American computer scientist and United States Navy rear admiral. One of the first programmers of the Harvard Mark I computer, she was a pioneer of computer programming who invented one of the first linkers. Hopper was the first to devise the theory of machine-independent programming languages, and the FLOW-MATIC programming language she created using this theory was later extended to create COBOL, an early high-level programming language still in use today. Wikipedia

Andy van Dam

Andy van Dam helped pioneer the field of computer graphics and coauthored three editions of the fundamental textbook used by most university computer science (CS) students who study computer graphics. He co-created a pioneering hypertext system and word processor in 1967; this and its successors helped provide inspiration for today's world wide web. He also cofounded the precursor to SIGGRAPH, the professional society for computer graphics. In the 1970s and 1980s, he played key roles in pioneering the use of computers in education, including what is now called digital humanities. Over his five-decade career teaching at Brown University, van Dam has taught over 10,000 students, many of whom went on to make major contributions to computer graphics and its uses in areas as diverse as scientific visualization and entertainment, hyper/multimedia, and the online world.

Instead of a single "inventor", the personal computer ecosystem and the Internet were developed by many people over many years, as you can see from some of the names above. The following links show are some of those already called out and some additional Internet pioneers who contributed to its early and ongoing development. These include early theoretical foundations, specifying original protocols, and expansion beyond a research tool to wide public deployment.

More Internet pioneers here:

https://icannwiki.org/Internet_Hall_of_Fame

https://en.wikipedia.org/wiki/List_of_Internet_pioneers

https://icannwiki.org/ARPANET